Meridian 1

X11 Release 25.40

Succession Communication Server for Enterprise 1000

X21 Release 2.0

IP Line

Description, Installation, and Operation

Document Number: 553-3001-204
Document Release: Standard 4.00
Date: November 2002

Printed in Canada

Revision history

November 2002

Standard 4.00. This document is up-issued to support IP Line 3.0 on Meridian 1, Release 25.40 and Succession Communication Server for Enterprise 1000, Release 2.0.

March 2002

Standard 3.00.

January 2002

Standard 2.00. Not Released.

June 2001

Standard 1.00

Contents

About this Document

Subject

This document describes the physical and functional characteristics of the Meridian 1 and Succession Communication Server for Enterprise 1000 IP Line 3.0 application and its use on the Voice Gateway Media Cards. This document also explains how to engineer, install, configure, administer, and maintain an IP Telephony node that contains Voice Gateway Media Cards.

Applicable systems

This document applies to a Meridian 1 large system (Option 51C, 61C, or 81C), a Meridian 1 small system (Option 11C or 11C Mini), and a Succession Communication Server for Enterprise (CSE) 1000 system. For the purposes of this document, all these systems are referred to generically as “system.”

Structure and conventions

This document has separate chapters which are applicable only to either Optivity Telephony Manager (OTM) or Succession CSE 1000 Element Management.

The configuration, administration, and maintenance sections are divided into three chapters each. For example, there is a generic configuration chapter dealing with tasks related to installing and configuring IP Line. This chapter is followed by two other configuration chapters, one for OTM and another for Element Management. The administration and maintenance chapters have the same format.

The “Installation and Configuration Summary” chapter contains a summary of the steps for installing the Meridian 1 Rel 25.30 and Succession CSE 1000 Rel 1.1 systems (see page 200) and the Succession CSE 1000 Rel 2.0 systems (see page 204).

Description

Contents

This section contains information on the following topics:

Reference list

The following are the references for this section:

- *Internet Terminals Description* (553-3001-217)
- *Element Management* (553-3023-222)

Overview

IP Line 3.0 application provides an interface between an Internet Telephone and the Meridian 1 PBX / Succession Communication Server for Enterprise (CSE) 1000 Call Server. The IP Line 3.0 application extends the functionality of the ITG Pentium (ITG-P) Line card and introduces the Succession Media Card, a 32-port card.

The new functionality of the IP Line 3.0 application includes:

- New i2002 Internet Telephone support
- New platform support for the Succession Media Card and Succession Signaling Server
- New user features
  (see Table 1 on page 21 for a list of supported features)
- Additional administration and supportability

A Dynamic Host Configuration Protocol (DHCP) server can be used to provide the required information to enable the Internet Telephone network connection and connect to the Voice Gateway Media Card.

> ***Note:*** An ITG-P Line Card or a Succession Media Card with the IP Line 3.0 application installed is known as a Voice Gateway Media Card.

The Internet Telephone uses the IP network to communicate with the Voice Gateway Media Card and the optional DHCP server. Figure 1 on page 18 shows a system block diagram of the Meridian 1 and Succession CSE 1000 Rel 1.1 system. Figure 2 on page 19 shows a diagram of the Succession CSE 1000 Rel 2.0 system.

Refer to the *Internet Terminals Description* (553-3001-217) for more information on the following Internet Telephones:

- i2002 Internet Telephone
- i2004 Internet Telephone
- i2050 Software Phone

Figure 1
Meridian 1 and Succession CSE 1000 Rel 1.1 System Architecture

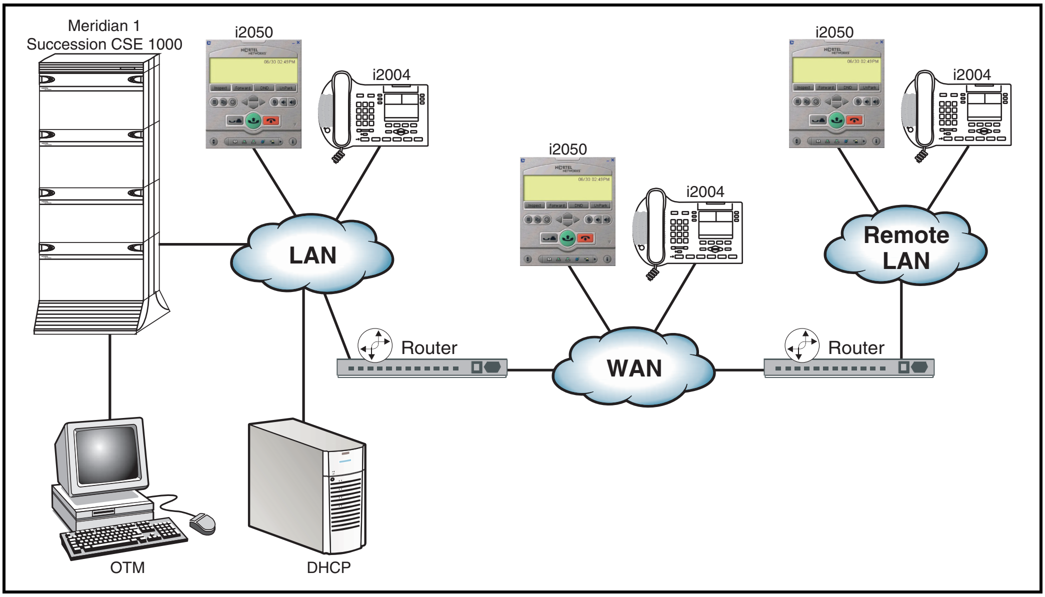
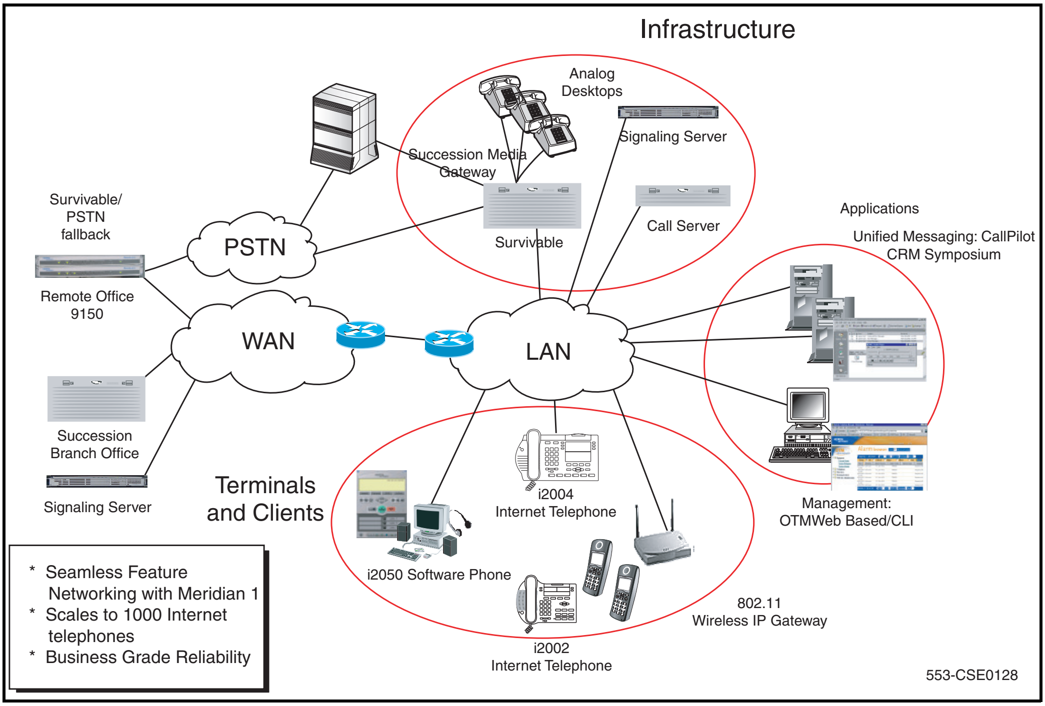


Figure 2
Succession CSE 1000 Rel 2.0 System Architecture



Applicable systems

The Meridian 1 and Succession CSE 1000 systems support the ITG-P Line Card and the Succession Media Card.

Unsupported products

The following remote service products do not support the ITG-P Line Card or Succession Media Card:

- Carrier Remote
- Mini-carrier Remote
- Fiber Remote
- Fiber Remote Multi-IPE

System requirements

Succession CSE 1000 Release 2.0 is the minimum system software that is required to have the complete functionality available in the IP Line 3.0 application loadware.

The IP Line 3.0 application is designed to run on Meridian 1 and Succession CSE 1000 systems. However, some of the new feature functionality requires changes to the PBX CPU software, as well as, to the IP Line application. As a result, the complete new feature functionality can be supported only on Succession CSE 1000 Release 2.0.

Some IP Line 3.0 application features are backward compatible with Meridian 1 Releases 25.15*, 25.30 and 25.40, and Succession CSE 1000 Release 1.1; however, not all the added functionality with Succession CSE 1000 Release 2.0 is available.

> ***Note:*** * Meridian 1 Rel 25.15 is supported only in the following regions: Europe, Middle East, and Africa (EMEA).

Table 1 on page 21 outlines the new features available for Succession CSE 1000 Release 2 and also shows the features which are backward compatible with previous systems. Also refer to "IP Line Feature Enhancements" on page 57 for information about these new features.

Table 1
IP Line 3.0 new feature support (Part 1 of 2)

Feature	CSE 1000 Rel 2.0	CSE 1000 Rel 1.1	Meridian 1 Rel 25.40 Meridian 1 Rel 25.30 Meridian 1 Rel 25.15[a]
Support of the i2002 Internet Telephone	Yes	No	No
Support for i2002/i2004 firmware version 1.3x	Yes	Yes (i2004 only)	Yes (i2004 only)
Succession Media Card Platform	Yes	Yes	Yes
Support for Signaling Server	Yes	No	No
NAT enhancement	Yes	Yes	Yes
Patching	Yes	Partial[b]	Partial[b]
802.1Q	Yes	Yes	Yes
Corporate Directory	Yes[c]	No	No
Data Path Capture tool	Yes	Yes	Yes
CSE Element Management support	Yes	No	No
Call statistics enhancements	Yes	No	No
User-defined Feature Key Labels	Yes	No	No
Private Zone	Yes	No	No
Graceful TPS Disable	Yes	Yes	Yes
Firmware download	Yes	Yes	Yes
Run-time download	Yes	Partial[d]	Partial[d]
Maintenance Audit Enhancement	Yes	Yes	Yes

Table 1
IP Line 3.0 new feature support (Part 2 of 2)

Feature	CSE 1000 Rel 2.0	CSE 1000 Rel 1.1	Meridian 1 Rel 25.40 Meridian 1 Rel 25.30 Meridian 1 Rel 25.15[a]
Watchdog Timer	Yes	Yes	Yes
Improved Login Banner and Password Guessing Protection	Yes	Partial[e]	Partial[e]

a. Meridian 1 Rel 25.15 is supported only in the following regions: Europe, Middle East, and Africa (EMEA).
b. Node level patching is not provided by OTM 2.0. The patching CLI command of the ITG-P Line Card and Succession Media Card can be used.
c. OTM 2.0 is required for the creation of the Corporate Directory database.
d. For more information, see “Run-time configuration changes” on page 82.
e. For more information, see “Login Banner Enhancement” on page 411 and “Password Guessing Protection” on page 412.

OTM and Element Management

Optivity Telephony Manager (OTM) 2.0 and CSE 1000 Element Management are used throughout this document as the primary interface for Voice Gateway Media Card and IP Line 3.0.

OTM 2.0 includes an application called "ITG Line 3.0" which is used to configure, administer, and maintain the IP Line on Meridian 1 and Succession CSE 1000 Release 1.1 systems. OTM 2.0 is the minimum required version.

CSE 1000 Element Management is the tool that is used as the configuration, administration, and maintenance interface for IP Line on the Succession CSE 1000 Release 2.0 system. CSE 1000 Element Management is referred to as Element Management for the remainder of this document.

Support of OTM's ITG Line 3.0 application

OTM's ITG Line 3.0 application fully supports IP Line 3.0 on the Meridian 1 Rels 25.15, 25.30, 25.40 and Succession CSE 1000 Rel 1.1 systems. OTM's ITG Line 3.0 application provides the feature set equivalent of the older ITG Line 2.2 application. IP Line 3.0 is not supported on systems prior to Release 25.15.

OTM's ITG Line 3.0 application provides limited functionality and support for Succession CSE 1000 Rel 2.0 systems. Instead, CSE 1000 Element Management is used for base line configuration of the Succession CSE 1000 Rel 2.0 systems. However, OTM 2.0 is required for Alarm Management and the Corporate Directory feature. OTM 2.0 also provides some Operational Measurement reporting.

> ***Note:*** Element Management does have some Operational Measurement report capabilities.

OTM 2.0 is the only management tool for IP Line on Meridian 1 Rel 25.xx and Succession CSE Rel 1.1 systems. Element Management is the primary management tool for Succession CSE 1000 Rel 2.0; however, OTM 2.0 does provide partial support.

Table 2 outlines the systems that use OTM's ITG Line 3.0 application for the configuration, administration, and maintenance of IP Line.

Table 2
Systems using OTM's ITG Line 3.0 application for IP Line management

Supported Release		The following systems use OTM's ITG Line 3.0 application for IP Line 3.0
Meridian 1	19	Not supported
	20	Not supported
	21	Not supported
	22	Not supported
	23	Not supported
	24	Not supported
	25.15	Mandatory
	25.30	Mandatory
	25.40	Mandatory
CSE 1000	1.0	Not supported
	1.1	Mandatory
	2.0	Limited support and functionality* (*Uses Element Management for majority of IP Line configuration.)

System configurations

IP Line 3.0 can be used on different system configurations and its use varies on different system configurations. There are three different systems configurations:

1 Succession CSE 1000 Rel 2.0 Normal configuration

2 Succession CSE 1000 Rel 2.0 Branch Office configuration

3 Meridian 1 and Succession CSE 1000 Rel 1.1 configuration

Succession CSE 1000 Rel 2.0 Normal configuration

In the Normal configuration, there is a Succession Signaling Server in the system. The Signaling Server is a server that provides signaling interfaces to the IP network. The Signaling Server provides a central processor to drive the signaling for Internet Telephone and IP Peer Networking.

With IP Line 3.0, the Terminal Proxy Server (TPS) executes on the Signaling Server card and the media gateway executes on the ITG-P Line Card or the Succession Media Card (the Voice Gateway Media Cards). All Internet Telephones register with the Signaling Server card. The Voice Gateway Media Cards provide just the gateway media access. The Signaling Server also acts as the Master for the node.

A backup Signaling Server can exist in the Normal configuration. If the primary Signaling Server fails, the backup Signaling Server takes over and all Internet Telephones reregister with the backup.

If the primary Signaling Server has no backup and the primary Signaling Server fails, one of the Voice Gateway Media Cards is elected to be the node Master. The Internet Telephones then register to the Voice Gateway Media Cards. The same is true if the backup Signaling Server fails.

Multiple nodes can be configured in Succession CSE 1000 Release 2.0. If there are multiple nodes, the primary node is the Signaling Server (the Leader and Master).

If additional nodes are configured on the system, the Voice Gateway Media Cards in these nodes operate the same as in ITG Line 2.0-2.2. That is, the card provides both the TPS and the voice gateway functionality. In each node, one Voice Gateway Media Card is configured as a Leader.

In a Succession CSE 1000 Rel 2.0 system, the Signaling Server (if it exists) is the Leader. If additional Signaling Servers exist, they are known as followers. If the Leader Signaling Server fails and a follower Signaling Server exists, then the “follower” Signaling Server becomes the Leader. In the unlikely event that the new Leader Signaling Server also fails, the Leader role is transferred to one of the Voice Gateway Media Cards. An election is held and one of the Voice Gateway Media Cards becomes the Master. The display on that card’s faceplate is Mxxx. When the Signaling Server comes back online, the mastership is transferred back to the Signaling Server. The Voice Gateway Media Card becomes a follower again and F000 is displayed on the card’s faceplate.

Succession CSE 1000 Rel 2.0 Branch Office configuration

In the Branch Office configuration, the Internet Telephones register first with the Branch Office TPS, then are redirected to the main office’s TPS.

If the connection to the main office is lost, the Internet Telephones register with the Branch Office TPS and continue to have service. The Internet Telephones have service because the telephones are configured with the node IP address of the Branch Office TPS.

For more information about this configuration, refer to the *Branch Office Guide* (553-3023-258).

Meridian 1 Rel 25.40 and Succession CSE 1000 Rel 1.1 configuration

In the Meridian 1 and Succession CSE 1000 Rel 1.1 configurations, there is no Signaling Server in the system. Each ITG-P Line Card and Succession Media Card functions as both a TPS and voice gateway. Since there is no Signaling Server in the system, the TPS functionality is on the card just as it is with ITG Line 2.0-2.2. In this configuration, one card is configured as the Leader and Internet Telephones register with individual Voice Gateway Media Cards.

Loadware delivery

IP Line 3.0 supports loadware delivery through the following formats:

1. CompactFlash
2. Signaling Server CD-ROM
3. Downloadable from the Nortel Networks Web site

Note: IP Line 3.0 loadware is no longer available through CD-ROM delivery.

The IP Line loadware and related documentation (such as *Readme First* documents) can be downloaded from the Nortel Networks Web site. See Appendix G on page 719 for details.

Required packages

The Internet Telephones require the software packages listed in Table 3.

Table 3
Required packages

Package	Package number
Digital Set Package (DSET)	88
Aries Terminal Package (ARIES)	170

Note: To configure the IP Line 3.0 in groups 5-7 on Option 81C, the Fiber Network (FIBN) software package #365 is required.

IP Line package components lists

Meridian 1 and Succession CSE 1000 Rel 1.1 package components

Table 4 lists the IP Line package components for the Meridian 1 and Succession CSE 1000 Rel 1.1 systems.

Table 4
Meridian 1 and Succession CSE 1000 Rel 1.1
IP Line 32-Port package components (Part 1 of 2)

Component	Code
Succession Media Card 32-Port - IP Line 3.0 Voice Gateway Systems Package for Meridian 1 and Succession CSE 1000 Rel 2.0, includes: • Succession Media Card 32-Port assembly (NTDU40BA) • Succession IP Line 3.0 Voice Gateway CompactFlash • ITG EMC Shielding Kit • Readme First Document • Shielded 50-pin to Serial/ELAN/TLAN adaptor • PC Maintenance cable • Succession IP Line 3.0 Voice Gateway NTP (CD-ROM) • ITG-specific Meridian 1 Backplane 50-pin I/O Panel Filter Connector (see Note)	NTDU41CA
Succession Media Card 32 Port assembly	NTDU40BA
ITG EMC Shielding Kit	NTVQ83AA
Shielded 50-pin to Serial/ELAN/TLAN Adaptor	A0852632
PC Maintenance cable	NTAG81CA

Table 4
Meridian 1 and Succession CSE 1000 Rel 1.1
IP Line 32-Port package components (Part 2 of 2)

Component	**Code**
ITG-specific Meridian 1 Backplane 50-pin I/O Panel Filter Connector (see Note)	NTCW84JA
Succession IP Line 3.0 Voice Gateway NTP (CD-ROM), includes: • *IP Line: Description, Installation and Operation* (553-3001-204) • *Internet Terminals Description* (553-3001-217) • *i2002 Internet Telephone User Guide* • i2002 Quick Reference Card • *i2004 Internet Telephone User Guide* • i2004 Quick Reference Card • *i2050 Software Phone User Guide*	NTDW81AD
Succession IP Line 3.0 Voice Gateway Internet Telephone User Guides & Quick Reference Guides (CD-ROM), includes • *i2002 Internet Telephone User Guide* • i2002 Quick Reference Card • *i2004 Internet Telephone User Guide* • i2004 Quick Reference Card • *i2050 Software Phone User Guide*	NTDW85AA
Note: The I/O panel filter connector is not required for Option 11C, Option 11C-Mini, or Succession CSE 1000.	

Succession CSE 1000 Rel 2.0 package components

Table 5 lists the IP Line package components for the Succession CSE 1000 Rel 2.0 system.

Table 5
Succession CSE 1000 Rel 2.0
IP Line 32-Port package components (Part 1 of 2)

Component	Code
Succession Media Card 32-Port - IP Line 3.0 Voice Gateway Systems Package for Succession CSE 1000 Rel 2.0, includes: • Succession Media Card 32-Port Assembly (NTDU40BA) • Succession IP Line 3.0 Voice Gateway CompactFlash • ITG EMC Shielding Kit • Readme First Document • Shielded 50-pin to Serial/ELAN/TLAN adaptor • Succession IP Line 3.0 Voice Gateway NTP (CD-ROM)	NTDU41BB
Succession Media Card 32 Port assembly	NTDU40BA
ITG EMC Shielding Kit	NTVQ83AA
Shielded 50-pin to Serial/ELAN/TLAN Adaptor	A0852632

Table 5
Succession CSE 1000 Rel 2.0
IP Line 32-Port package components (Part 2 of 2)

Component	Code
Succession IP Line 3.0 Voice Gateway NTP (CD-ROM), includes: • *IP Line: Description, Installation and Operation* (553-3001-204) • *Internet Terminals Description* (553-3001-217) • *i2002 Internet Telephone User Guide* • i2002 Quick Reference Card • *i2004 Internet Telephone User Guide* • i2004 Quick Reference Card • *i2050 Software Phone User Guide*	NTDW81AD
Succession IP Line 3.0 Voice Gateway Internet Telephone User Guides & Quick Reference Guides (CD-ROM), includes • *i2002 Internet Telephone User Guide* • i2002 Quick Reference Card • *i2004 Internet Telephone User Guide* • i2004 Quick Reference Card • *i2050 Software Phone User Guide*	NTDW85AA

Succession CSE 1000 Rel 2.0 Branch Office package components

Table 6 lists the IP Line package components for the Succession CSE 1000 Rel 2.0 Branch Office.

Table 6
Succession CSE 1000 Rel 2.0 Branch Office
IP Line 8-Port package components (Part 1 of 2)

Component	Code
Succession Media Card 8-Port - IP Line 3.0 Voice Gateway Systems Package for Succession CSE 1000 Rel 2.0 Branch Office, includes: • Succession Media Card 8-Port Assembly (NTDU40AA) • Succession IP Line 3.0 Voice Gateway CompactFlash • ITG EMC Shielding Kit • Readme First Document • Shielded 50-pin to Serial/ELAN/TLAN adaptor • Succession IP Line 3.0 Voice Gateway NTP (CD-ROM)	NTDU41AB
Succession Media Card 8 Port assembly	NTDU40AA
ITG EMC Shielding Kit	NTVQ83AA
Shielded 50-pin to Serial/ELAN/TLAN Adaptor	A0852632

Table 6
Succession CSE 1000 Rel 2.0 Branch Office
IP Line 8-Port package components (Part 2 of 2)

Component	Code
Succession IP Line 3.0 Voice Gateway NTP (CD-ROM), includes: • *IP Line: Description, Installation and Operation* (553-3001-204) • *Internet Terminals Description* (553-3001-217) • *i2002 Internet Telephone User Guide* • i2002 Quick Reference Card • *i2004 Internet Telephone User Guide* • i2004 Quick Reference Card • *i2050 Software Phone User Guide*	NTDW81AD
Succession IP Line 3.0 Voice Gateway Internet Telephone User Guides & Quick Reference Guides (CD-ROM), includes • *i2002 Internet Telephone User Guide* • i2002 Quick Reference Card • *i2004 Internet Telephone User Guide* • i2004 Quick Reference Card • *i2050 Software Phone User Guide*	NTDW85AA

Documentation

The following documents are available on the Succession IP Line 3.0 Voice Gateway NTP CD-ROM and on the Nortel Networks Web site:

- *IP Line: Description, Installation and Operation* (553-3001-204)
- *Internet Terminals Description* (553-3001-217)
- *i2002 Internet Telephone User Guide*
- i2002 Quick Reference Card
- *i2004 Internet Telephone User Guide*
- i2004 Quick Reference Card
- *i2050 Software Phone User Guide*

The documents are also available from SERL (Succession Electronic Reference Library).

Voice Gateway Media Card description

Voice Gateway Media Card is a term used to encompass both the ITG-P Line Card and the Succession Media Card. These cards plug into an Intelligent Peripheral Equipment (IPE) shelf in the Meridian system and into a Media Gateway and Media Gateway Expansion in the Succession CSE 1000 Rel 2.0 system.

The ITG-P Line card (NTVQ55AA) occupies two slots while the Succession Media Card (NTVQ01BA) occupies only one slot. The Succession Media Card comes in two versions: 8-port and 32-port.

The Succession Media Card introduces the following features:

- It increases the packet processing power compared to that of the ITG-P Line card.
- It increases the channel density from 24 to 32 ports (for 32-port version).
- It reduces the slot count from a dual IPE slot to a single IPE slot.
- It supports up to 128 Internet Telephones for 32-port version, while 32 Internet Telephones are supported on the 8-port version.

The 8-port version is typically intended for the Branch Office configuration. The 8-port Succession Media Card can be upgraded to the 32-port version using a DSP card installation.

Table 7 on page 36 provides a comparison of the ITG-P Line Card and Succession Media Cards. The tables also shows a comparison of the 8-port and 32-port Succession Media Card.

Table 7
Comparison of ITG-P Line Card and Succession Media Card

Item	ITG-P Line Card	Succession Media Card (32 port)	Succession Media Card (8 port)
Total DSP Channels	24	32	8
Number of slots the card occupies	2	1	1
Operating System	VxWorks 5.3	VxWorks 5.4	VxWorks 5.4
Processor	Pentium	IXP1200	IXP1200
DSP	8 x TI5409	4 x TI5421	1 x TI5421
Telogy version	7.01	8.1 High Density version (8 ports for each DSP)	8.1 High Density version (8 ports for each DSP)
Number of Internet Telephones on each Voice Gateway Media Card	96	128	32
Image file name prefixes shown by swVersionShow command	IPL P	IPL SA	IPL SA
/C: drive	On board Flash 2 x 4Mb	Plug-in CompactFlash 16Mb	Plug-in CompactFlash 16Mb
Upgrade	Two images files	One image file (no backup)	One image file (no backup)

Voice Gateway Media Cards have an ELAN management Ethernet port (10BaseT) and a TLAN VoIP Ethernet port (10/100BaseT) on the I/O panel.

> ***Note:*** ELAN or Embedded LAN is for isolation of critical telephony signaling between the Call Server and the other components. ELAN is also known as the Management LAN. TLAN or Telephony LAN is for telephony / voice / signaling traffic. The TLAN connects to the customer network and the rest of the world. TLAN is also known as the Voice LAN.

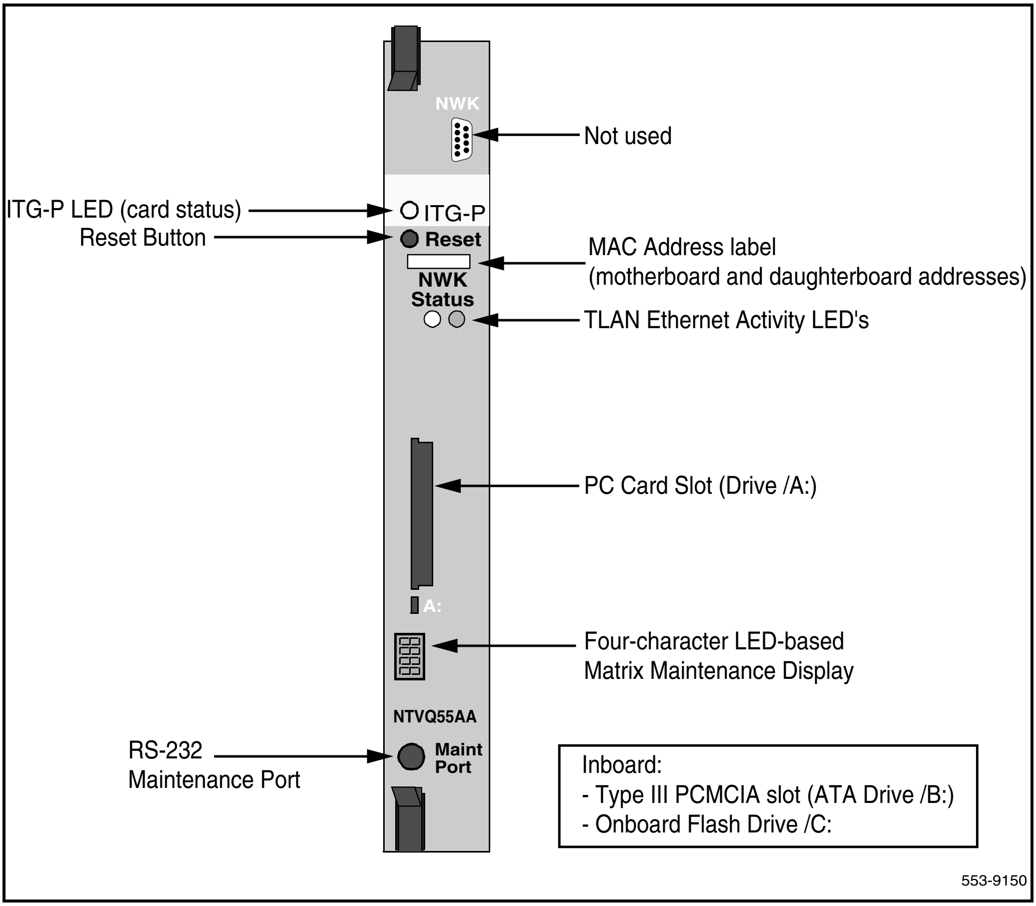
There is an RS-232 Maintenance Port connection on the faceplates of both the ITG-P Line Card and the Succession Media Card. The ITG-P Line Card has an alternative connection to the same serial port on the I/O backplane.

CAUTION
Do not connect maintenance terminals to both the faceplate and the I/O panel serial maintenance port connections at the same time.

ITG-P Line Card controls, indicators, and connectors

Figure 3 on page 38 shows the ITG-P Line Card faceplate components. The information in this section describes the components.

Figure 3
ITG-P Line Card (NTVQ55AA) assembly



Faceplate components

The components on the faceplate of the ITG-P Line Card are described in the following sections.

NWK

The faceplate connector labeled NWK is a 9-pin, sub-miniature D-type connector. The connector is not used for the IP Line application.

> **WARNING**
> The NWK connector looks like a 9-pin serial connector. DO NOT connect a serial cable or any other cable to it. If you install a cable to the NWK connector, the TLAN is disabled.

ITG-P LED (card status)

The red status faceplate LED indicates the enabled/disabled status of the 24 card ports. The LED is on (red) during the power-up or reset sequence. The LED remains lit until the card is enabled by Meridian 1 or Succession CSE 1000. If the LED remains on, the self-test failed, the card is disabled, or the card rebooted.

Reset Button

Press the Reset switch to reset the card without having to cycle power to the card. This switch is normally used after a card loadware upgrade to the card or to clear a fault condition.

MAC Address label

The MAC Address label on the card's faceplate shows the motherboard and daughterboard addresses. The ELAN address corresponds to the Management MAC address. The Management MAC address for each card is assigned during manufacturing and is unchangeable. The ELAN/Management MAC address is the MOTHERBOARD Ethernet address found on the label. The MAC Address label on the ITG-P Line Card is similar to the following:

ETHERNET ADDRESS
MOTHERBOARD
00:60:38:8c:03:d5
DAUGHTERBOARD
00:60:38:01:b3:cb

TLAN Ethernet Activity LEDs (labeled NWK Status LEDs)

The NWK Status LEDs display the TLAN Ethernet activity.

- Green - The LED is on if the carrier (link pulse) is received from the TLAN Ethernet switch.
- Yellow - The LED flashes when there is TLAN data activity. During heavy traffic, the yellow LED can stay continuously lit.

Note: There are no Ethernet status LEDs for the ELAN management interface.

PC Card Slots

The ITG-P Line Card has one faceplate PC Card slot (designated Drive /A:). It is used for optional maintenance. The ITG-P Line Card also has one unused inboard slot (designated Drive /B:). The PC card slots support high-capacity PC flash memory cards.

Matrix Maintenance Display

A four-character, LED-based dot matrix display shows the maintenance status fault codes and other card state information.

RS-232 Maintenance Port (Maint Port)

The ITG-P Line Card faceplate provides a female 8-pin mini-DIN serial maintenance port connection (labeled Maint Port). An alternative connection to the faceplate serial maintenance port exists on the NTMF94EA I/O panel breakout cable.

CAUTION
Do not connect maintenance terminals or modems to the faceplate and I/O panel DB-9 male serial maintenance port at the same time.

Backplane interfaces

The backplane connector provides ELAN, TLAN, alternate connection to the serial maintenance port DS-30X and Card LAN interfaces.

DS-30X voice/signaling

DS30X carries Pulse Code Modulation (PCM) voice and proprietary signaling on the IPE backplane between the ITG-P Line Card and the Intelligent Peripheral Equipment Controller (XPEC).

Card LAN

Card LAN carries card polling and initialization messages on the IPE backplane between the ITG-P Line Card and the Intelligent Peripheral Equipment Controller (XPEC).

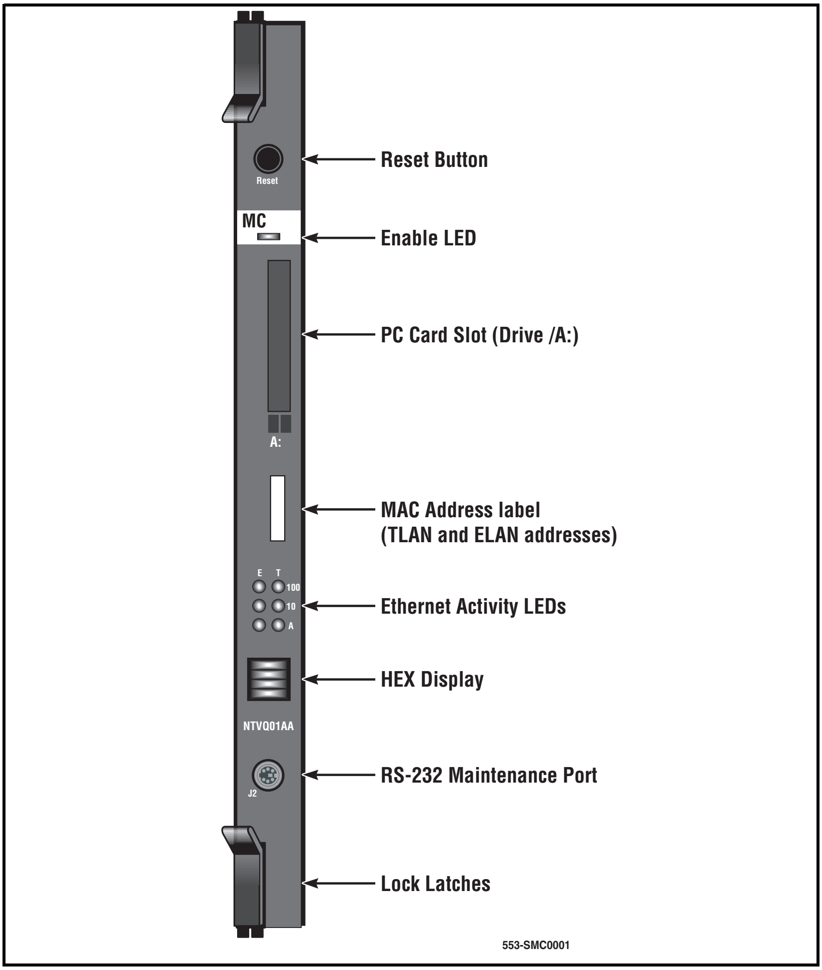
Assembly description

The ITG-P Line Card assembly is a two-slot motherboard and daughterboard combination. A PCI interconnect board connects the ITG motherboard and the DSP daughterboard.

Succession Media Card controls, indicators, and connectors

Figure 4 on page 42 shows the Succession Media Card faceplate.

Figure 4
Succession Media Card (NTVQ01BA or NTVQ01AA) assembly



Faceplate components

The components on the faceplate of the Succession Media Card are described in the following sections.

Reset Button

Use the Reset button on the faceplate to manually reset the Succession Media Card. This enables the card to be reset without cycling power to it. The Reset button is used to reboot the card after a loadware upgrade or to clear a fault condition.

Enable LED

The faceplate red LED indicates the following:

- the enabled/disabled status of the card
- the self-testing result during power up or card insertion into an operational system

PC Card Slot

This slot accepts the Type I or Type II standard PC Flash Cards, including ATA Flash cards (3 Mb to 170 Mb). The slot is labeled /A:.

Nortel Networks supplies PC Card adaptors that enable CompactFlash cards to be used in the slot.

MAC Address label

The MAC Address label on the card's faceplate is labeled ETHERNET ADDRESS. It shows the TLAN and ELAN addresses. The ELAN address corresponds to the cards Management MAC address. The Management MAC/ELAN address for each card is assigned during manufacturing and is unchangeable. The MAC Address label on the Succession Media Card is similar to the following:

ETHERNET ADDRESS
TLAN
00:60:38:BD:C9:9C
ELAN
00:60:38:BD:C9:9D

Ethernet Activity LEDs

The faceplate contains six Ethernet activity LEDs, three for the ELAN network and three for the TLAN network. The LEDs indicate the following links on the ELAN and TLAN (in order from the top):

1 100 (100BaseT)

2 10 (10BaseT)

3 A (Activity)

Maintenance Hex display

This is a four-digit LED-based hexadecimal display that provides the role of the card. It also provides an indication of fault conditions and the progress of PC card-based loadware upgrades or backups.

RS-232 Maintenance Port

The Succession Media Card faceplate provides a female 8-pin mini-DIN serial maintenance port connection. The faceplate on the card is labeled J2.

Functional description of the Voice Gateway Media Cards

The ITG-P Line Card and Succession Media Card can perform the following two separate functions depending on the system in which the card is located:

- It acts as a gateway between the circuit-switched voice network and the IP network.
- It acts as Terminal Proxy Server (TPS) or “virtual line card” for the i2002/i2004 Internet Telephones and i2050 Software Phone.

Gateway functional description

The Gateway:

- registers with the PBX using the TN Registration messages
- accepts commands from the PBX to connect/disconnect audio channel
- uses RTP/RTCP protocol to transport audio between the gateway and the Internet Telephone
- encodes/decodes audio from PCM to and from the Internet Telephone's format
- provides echo cancellation for the speaker on the i2002 and i2004 Internet Telephones (not applicable to the i2050 Software Phone)

Meridian 1 Rel 25.30 and Succession CSE 1000 Rel 1.1

Each ITG-P Line Card and Succession Media Card functions as both the LTPS and Voice Gateway, just as it did with ITG Line 2.0-2.2.

The Gateway portion of the card connects to the Meridian 1 or Succession CSE 1000 Rel 1.1 through the DS30X backplane. The Gateway portion also receives call speech path setup and codec selection commands through the ELAN port. The Internet Telephone connects to both the Gateway and the TPS functions through the TLAN port.

Succession CSE 1000 Rel 2.0

A Signaling Server is always present in the system. The LTPS executes on the Signaling Server card and the media gateway executes on the ITG-P Line Card or Succession Media Card. The Voice Gateway Media Cards provide only the gateway media access.

Virtual superloops, virtual TNs, and physical TNs

Virtual TNs (VTNs) enable configuration of service data for an Internet Telephone, such as key layout and class of service, without requiring the Internet Telephone to be dedicated (hard-wired) to a given TN on the Meridian 1 and Succession CSE 1000 Voice Gateway Media Card.

Calls are made between an Internet Telephone and circuit-switched telephone/trunks using the full Meridian 1 and Succession CSE 1000 feature set. Digital Signal Processor (DSP) channels are allocated dynamically for this type of call to perform the encoding/decoding required to connect the Internet Telephone to the circuit-switched network.

To create an Internet Telephone using VTNs, you must create a virtual superloop in LD 97.

- Up to 1024 VTNs can be configured on a single virtual superloop for Option 51C/61C/81/81C.
- Up to 128 VTNs can be configured on a single virtual superloop for Option 11C/11C-Mini, leading to a maximum number of 640 VTNs for each Option 11C/11C-Mini.
- Up to 128 VTNs can be configured on a single virtual superloop for Succession CSE 1000 Rel 1.0 and Rel 1.1
- Up to 1024 VTNs can be configured on a single virtual superloop for Succession CSE 1000 Rel 2.0. Table 8 on page 47 describes the virtual superloop and virtual card mapping on a Succession CSE 1000 Rel 2.0 system. Each superloop has two ranges of cards.

Table 8
Virtual superloop/virtual card mapping for Succession CSE 1000 Rel 2.0

SUPL	Card	
96	61-64	81-84
100	65-68	85-88
104	69-72	89-92
108	73-76	93-96
112	77-80	97-99

Each ITG-P Line card provides 24 physical TNs and the Succession Media Card provides 32 physical TNs. The physical TNs are the gateway channels (DSP ports). Configure the physical TNs (IPTN) in LD 14. They appear as tie trunks without a route data block.

Virtual TNs

Virtual TNs enable you to configure service data for a terminal, such as key layout and class of service, without requiring a physical terminal to be directly connected to the PBX/Call Server.

The concentration of Internet Telephones is made possible by dynamically allocating a port (also referred to as a physical TN) of the Voice Gateway Media Card for a circuit-switched to Internet Telephone call. All Meridian 1 and Succession CSE 1000 speech path management is done with physical TNs instead of the virtual TNs.

The channels (ports) on the Voice Gateway Media Cards are pooled resources.

The Internet Telephones (virtual TNs) are defined on virtual superloops.

A virtual superloop is a hybrid of real and phantom superloops. Like phantom superloops, no hardware (for example, XPEC or line card) is used to define and enable units on a virtual superloop. As with real superloops, virtual superloops use the time slot map to handle Internet Telephone (virtual TNs) to Internet Telephone calls.

Internet Telephone registration

The Terminal Proxy Server (TPS) maintains a count of the number of telephones registered to the card. Each IP Telephony node has one active Master. The active Master broadcasts to all Voice Gateway Media Cards and requests a response if it has room for another telephone.

The Election function uses a selection process to determine the node's Master. The Census function determines the Voice Gateway Media Cards within an IP Telephony node.

The maximum number of telephones for each ITG-P Line Card is 96 and the maximum number of telephones for each Succession Media Card is 128.

> ***Note:*** The Succession Media Card is available in two versions: an 8-port card or a 32-port card. If the Succession Media Card has the 8-port configuration (that is, the DSP daughterboard in not installed), then the maximum number of telephones is 32.

Succession CSE 1000 Rel 2.0 registration

With Succession CSE 1000 Rel 2.0, the Internet Telephones register with the TPS on the Signaling Server. If a secondary Signaling Server exists, the Internet Telephone registrations are split between the primary and secondary Signaling Servers to aid in load balancing. In this case, the Internet Telephone registrations alternate between the primary and secondary Signaling Servers.

If the primary Signaling Server fails, the secondary Signaling Server takes over (if it exists) and the Internet Telephones register with the TPS on the secondary Signaling Server. If the secondary Signaling Server does not exist or in the case of failure of the secondary Signaling Server, the Internet Telephones register with the TPS functionality on the Voice Media Gateway Cards.

For more information on Signaling Server failure and redundancy, see *Planning and Engineering Guidelines* (553-3023-102).

Meridian 1 and Succession CSE 1000 Rel 1.1 registration

With Meridian 1 and Succession CSE 1000 Rel 1.1, the Internet Telephones register with the TPS on the individual Voice Gateway Media Cards (as there is no Signaling Server within these systems). The Voice Gateway Media Cards (ITG-P Line Cards and Succession Media Cards) include both the TPS and the voice gateway functionality.

If a Voice Gateway Media Card has Internet Telephones registered on it and the card fails, the Internet Telephones re-register with another Voice Gateway Media Card.

Virtual Terminal Manager description

The Virtual Terminal Manager (VTM):

- Arbitrates application access to the Internet Telephones.
- Manages all the telephones between the applications and the stimulus messaging to the telephone.
- Maintains context-sensitive states of the telephone (for example, display or lamp state).
- Isolates telephone-specific information from the applications (for example, the number of display lines, number of characters for each display line, tone frequency, and cadence parameters).

Interactions with Internet Telephones

The Internet Telephone receives the IP address of the Connect Server through either DHCP or manual configuration. The Internet Telephone contacts the Connect Server that instructs the Internet Telephone to display a message on its display screen requesting the customer's IP Telephony node number and TN.

After the node number and TN are entered, the Internet Telephone contacts the Node Master which selects a TPS with sufficient capacity to register the Internet Telephone. The chosen TPS contacts the Internet Telephone and, if the Internet Telephone is valid, registers it with the Meridian 1 or Succession CSE 1000. The registration information is then saved to the Internet Telephone.

Unregistration

If the Voice Gateway Media card detects a loss of connection with one of its registered Internet Telephones, it logs the event and sends an unregister message to the Meridian 1 or Succession CSE 1000 for that Internet Telephone.

Signaling and messaging

The IP Line application sends Scan and Signaling Distribution (SSD) messages through the Meridian 1 or Succession CSE 1000 ELAN. When tone service is provided, it is signaled to the TPS using new SSD messages sent through the ELAN.

Signaling protocols

The signaling protocol between the Internet Telephone and the IP Telephony node is the Unified Networks IP Stimulus Protocol (UNIStim). The Reliable User Datagram Protocol (RUDP) is the transport protocol.

RUDP

RUDP is used for ELAN communications between the Meridian 1 or Succession CSE 1000 CPU and the Voice Gateway Media Cards, and for TLAN communications between the IP Telephony node and the Internet Telephones.

Signaling messages between the Voice Gateway Media Card and Internet Telephones use RUDP. Each RUDP connection is distinguished by its IP address and port number. RUDP is another layer on top of UDP. RUDP is proprietary to Nortel Networks.

The features of RUDP are:

- reliable communication system over a network
- packages are resent if an acknowledgement message (ACK) is not received following a time-out
- messages arrive in the correct sequence

- duplicate messages are ignored
- loss of contact detection

When a data sequence is packetized and sent from source **A** to receiver **B**, RUDP adds a number to each packet header to indicate its order in the sequence.

- If the packet is successfully transmitted to **B**, **B** sends back an ACK to **A**, acknowledging that the packet has been received.
- If **A** receives no message within a configured time, it retransmits the packet.
- If **B** receives a packet without having first received its predecessor, it discards the packet and all subsequent packets, and a NAK (no acknowledge) message which includes the number of the missed packet is sent to **A**. **A** retransmits the missed packet and continues.

UNIStim

The Unified Network IP Stimulus protocol (UNIStim) is the single point of contact between the various server components and the Internet Telephone.

UNIStim is the stimulus-based protocol used for communication between an Internet Telephone and a Terminal Proxy Server on the Voice Gateway Media Card.

ELAN TCP Transport

Although TCP is used for the signaling protocol between the Call Server and the Voice Gateway Media Card, RUDP remains for the Keep Alive mechanism for the link. This means RUDP messages are exchanged to maintain the link status between the Call Server and the Voice Gateway Media Card.

There is no change on the TLAN signaling mechanism. Internet Telephones continue to use the RUDP transport protocol to communicate with the Voice Gateway Media Card.

The TCP protocol enables messages to be bundled. Unlike the RUDP transport that creates a separate message for every signaling message (such as display updates or key messages), the TCP transport bundles a number of messages and sends them as one packet.

Handshaking is added to the Call Server and IP Line loadware so that the TCP functionality is automatically enabled. A loadware version check is performed by the IP Line application each time before it attempts to establish a TCP link with the Meridian 1 and Succession CSE 1000 CPU. If the version does not satisfy the minimum supported version (Meridian 1 Rel 25.40 or Succession CSE 1000 Rel 1.1), a RUDP link is used instead.

For Meridian 1 Rel 25.40 and Succession CSE 1000 Rel 1.1 systems, TCP transports messages, while RUDP establishes and maintains the link. However, for Meridian 1 Rel 25.15 or Rel 25.30, RUDP is used to maintain the link and all signaling.

Zones

To optimize IP Line traffic bandwidth use between different locations, the IP Line network is divided into “zones” representing different topographical areas of the network. All Internet Telephones and IP Line ports are assigned a zone number indicating the zone to which they belong.

When a call is made, the codecs used vary depending on which zone(s) the caller and receiver are in.

By default, when a zone is created in LD 117:

- codecs are selected to optimize voice quality (BQ - Best Quality) for connections between units in the *same* zone.
- codecs are selected to optimize voice quality (BQ - Best Quality) for connections between units in *different* zones.

Each zone can be configured to:

- optimize either voice quality or bandwidth usage for calls between users in that zone.
- optimize either voice quality or bandwidth usage within a zone and all traffic going out of a zone.

See "VoIP bandwidth management zones" on page 164.

For more information about zones, refer to the following:

- Shared and Private zones (see "Private Zone Configuration" on page 73)
- Zones and Virtual Trunks (see *Meridian 1 Integrated Telephony Gateway Trunk 2.0/ISDN Signaling Link: Description, Installation, and Operation* (553-3001-202))
- Zones and Branch Office (see *Branch Office* (553-3023-221))

Administration

The Voice Gateway Media Card is administered using multiple management interfaces including:

- a Graphical User Interface (GUI) provided by OTM 2.0 called ITG Line 3.0.
- a Command Line Interface (CLI).
- administration and maintenance overlays of Meridian 1 and Succession CSE 1000 Call Servers.
- a Web browser interface provided by Element Management. Element Management is used for administering Voice Gateway Media Cards in the Succession CSE 1000 Rel 2.0 systems.

  Note: Element Management is not available for earlier systems (Meridian 1 and Succession CSE 1000 Rel 1.1).

OTM 2.0's IP Line 3.0 application

For Meridian 1 systems, OTM 2.0 is required for IP Line 3.0. OTM is used for tasks such as the following:

- creating a node
- adding Voice Gateway Media Cards to the node
- transmitting loadware to the Voice Gateway Media Cards
- upgrading loadware

- defining SNMP alarms
- selecting codecs

Element Management

The Element Management Web server is required for Succession CSE 1000 Rel 2.0. Element Management enables the IP Line 3.0 application to be configured from a Web browser interface.

The “CSE 1000 Element Management” Web interface is used to manage the IP Line 3.0 application.

The Element Management Web interface is divided into two categories:

1. CSE 1000 Element Management - used to manage the Call Server and IP Telephony nodes (IP Line).
2. Gatekeeper Element Management - used to administer network numbering plan for Network Connect Server that is used by network-wide Virtual Office and Branch Office.

Command Line Interface

The Command Line Interface (CLI) provides a text-based interface to perform some specific Signaling Server and Voice Gateway Media Card installation, configuration, administration, and maintenance functions. You can establish a CLI session by connecting a TTY or PC to the card serial port or Telnet through the ELAN or TLAN IP address.

In the case of an IP Telephony node with no Signaling Server, the CLI must be used to configure the Leader card of the IP Telephony node so that OTM and Element Management can communicate with the Leader card and the node.

For more information about the CLI commands, see page 567.

Overlays

The following sections describe the changes that have been made to the Overlays with the introduction of IP Line 3.0.

LD 11

A new subtype for the i2002 Internet Telephone is introduced in LD 11. Also, the new CLS for the new Virtual Office feature has been added. The CLS prompt includes the VOLA/VOLD (Virtual Office Login Allowed/Denied) and VOUA/VOUD (Virtual Office User Allowed/Denied) for Virtual Office. LD 11 needs to accept CRPA/CRPD class of service input for the Corporate Directory feature on the Internet Telephones.

There are new prompts and responses available with LD 11. See Table 61: "LD 11 Configure an Internet Telephone" on page 263.

LD 14

There are two minor changes to the administration of the Voice Gateway Media Cards in LD 14. See "Configure physical TNs (LD 14)" on page 253 for the new responses (XTRK and MAXU). See Table 55: "Configure physical TNs in LD 14" on page 253 for prompts and responses.

LD 20

No new prompts have been added to LD 20. For the TYPE prompt, the I2002 response is introduced as a new customer response.

LD 81

Two changes have been made to LD 81. The FEAT prompt prints for the i2002 Internet Telephone and the FEAT prompt accepts VOLA, VOLD, VOUA, and VOUD for the new Virtual Office feature.

LD 82

No new prompts have been added to LD 83 however the i2002 Internet Telephone is printed.

Note: For a complete listing of the changes to the software input/output prompts, see *What's New for Succession Communication Server for Enterprise 1000* (553-3023-015).

IP Line Feature Enhancements

Contents

This section contains information on the following topics:

Reference list

The following are the references for this section:

- *i2002 Internet Telephone User Guide*
- *Internet Terminals Description* (553-3001-217)
- *Installing and Configuring Optivity Telephony Manager* (553-3001-230)
- *Features and Services* (553-3001-306)
- *Branch Office* (553-3023-221)
- *Element Management* (553-3023-222)
- *Maintenance* (553-3023-510)

Overview

The IP Line 3.0 application introduces a number of new feature enhancements. Table 9 lists these new features and the systems that support the new feature.

Table 9
IP Line 3.0 new feature support (Part 1 of 2)

Feature	CSE 1000 Rel 2.0	CSE 1000 Rel 1.1	Meridian 1 Rel 25.40 Meridian 1 Rel 25.30 Meridian 1 Rel 25.15[a]
Support of the i2002 Internet Telephone	Yes	No	No
Support for i2002/i2004 firmware version 1.3x	Yes	Yes (i2004 only)	Yes (i2004 only)
Succession Media Card Platform	Yes	Yes	Yes
Support for Signaling Server	Yes	No	No
NAT enhancement	Yes	Yes	Yes
Patching	Yes	Partial[b]	Partial[b]

Table 9
IP Line 3.0 new feature support (Part 2 of 2)

Feature	CSE 1000 Rel 2.0	CSE 1000 Rel 1.1	Meridian 1 Rel 25.40 Meridian 1 Rel 25.30 Meridian 1 Rel 25.15[a]
802.1Q	Yes	Yes	Yes
Corporate Directory	Yes[c]	No	No
Data Path Capture tool	Yes	Yes	Yes
CSE Element Management support	Yes	No	No
Call statistics enhancements	Yes	No	No
User-defined Feature Key Labels	Yes	No	No
Private Zone	Yes	No	No
Graceful TPS Disable	Yes	Yes	Yes
Firmware download	Yes	Yes	Yes
Run-time download	Yes	Partial[d]	Partial[d]
Maintenance Audit Enhancement	Yes	Yes	Yes
Watchdog Timer	Yes	Yes	Yes
Improved Login Banner and Password Guessing Protection	Yes	Partial[e]	Partial[e]

a. Meridian 1 Rel 25.15 is supported only in the following regions: Europe, Middle East, and Africa (EMEA).
b. Node level patching is not provided by OTM 2.0. The patching CLI command of the ITG-P Line Card and Succession Media Card can be used.
c. OTM 2.0 is required for the creation of the Corporate Directory database.
d. For more information, see “Run-time configuration changes” on page 82.
e. For more information, see “Login Banner Enhancement” on page 411 and “Password Guessing Protection” on page 412.

Feature Enhancements

Support of the i2002 Internet Telephone

The IP Line 3.0 application supports three telephones:

- the new i2002 Internet Telephone
- the i2004 Internet Telephone
- the i2050 Software Phone

The i2002 Internet Telephone is similar in appearance and functionality to the i2004 Internet Telephone; however, the i2002 has a smaller display and less feature keys.

Table 10 on page 61 shows a comparison of the i2002 and i2004 Internet Telephones.

For detailed information about the i2002 Internet Telephone, see the following Guides:

- *i2002 Internet Telephone User Guide*
- *Internet Terminals Description* (553-3001-217)

Table 10
Comparison of the i2002 and i2004 Internet Telephones

Feature	i2004 Internet Telephone	i2002 Internet Telephone
Display		
Display size and format	3 line display 24 characters on each line	1 line display of 24 characters
Information Line	3 * 24 characters	1 * 24 characters
Dedicated Data/Time field	Yes	No
Context Label field	Yes	No
Keys		
Soft Keys	4 soft keys, soft-labeling 7 characters long	4 soft keys, soft-labeling 6 characters long
Feature Keys	6 soft keys, soft-labeling 10 characters long	4 soft keys, soft-labeling 10 characters long
Other features		
Feature set	Based on the M2616 with select M3900 features added	Based on the M2616 with select M3900 features added
DHCP support	Yes	Yes
Transducers	Headset (HS) / Handset (HD) / Handsfree (HF)	Headset (HS) / Handset (HD) / Handsfree (HF)
Voice Codec support	G.711, G729A, G729AB, G.723.1[a]	G.711, G729A, G729AB, G.723.1[a]
Firmware download	Automatic firmware version checking and download	Automatic firmware version checking and download
3-port unmanaged Layer 2 switch for data and voice	Depending on the model, the switch can be added on externally or built-in	Built-in

a. The G.723.1 codec is supported only on Succession Communication Server for Enterprise (CSE) 1000 Rel. 2.0.

Corporate Directory

The new Corporate Directory feature is based on the M3900 telephone Corporate Directory feature and is available on the i2002 Internet Telephones, i2004 Internet Telephones, and the i2050 Software Phone.

The Corporate Directory database is created using OTM 2.0 and is generated from one of the following:

- the configured DN information from the Call Server
- the data from a corporate LDAP server

The database is downloaded and stored on the Call Server. It is then accessible to the Internet Telephones.

The Directory key on the telephone is used to access the directory, select a listing, and then dial a number from the Corporate Directory. The Navigation keys are used to refine the search within the Corporate Directory.

Corporate Directory is configured in LD 11. LD 11 needs to accept CRPA/CRPD class of service for the Internet Telephones (see "Corporate Directory: LD 11 configuration" on page 443).

In the Meridian 1 or Succession CSE 1000 Rel 1.1 configuration, the TPS is on the Voice Gateway Media Card. The ITG-P Line Card supports the registration of 96 Internet Telephones and the Succession Media Card supports the registration of 128 Internet Telephones. Both cards provide the Corporate Directory feature to all registered Internet Telephones.

In the Succession CSE 1000 Rel 2.0 Normal configuration, the TPS is on the Signaling Server. Each Corporate Directory entry requires 500 bytes of memory, therefore, with sufficient memory the Signaling Server can support Corporate Directory access from the same number of telephones that are registered.

For more information about the operation of the Corporate Directory feature, refer to:

- *Installing and Configuring Optivity Telephony Manager* (553-3001-230)
- *Internet Terminals Description* (553-3001-217).

CSE 1000 Element Management support

CSE 1000 Element Management is a new feature of the Succession CSE 1000 Rel 2.0 product that enables configuration of IP Line 3.0 using a Web browser.

With the introduction of Succession CSE 1000 Rel. 2.0, each Signaling Server is the host of a new Web server, CSE 1000 Element Management, that enables users to perform configuration, administration, and maintenance of the system components. CSE 1000 Element Management is a graphical Web interface and it provides a graphical alternative to the traditional Overlays and Command Line Interface. The interface is available to users running a Web browser on their computer. No special client software is required.

The Element Management Web server runs on each Signaling Server and the Signaling Server acts as a file server.

When a Web browser is opened and the IP address of the Signaling Server is entered, the Element Management interface is displayed. Element Management is then used to perform tasks such as configuring an IP Telephony node; checking and uploading loadware and firmware files; and retrieving the CONFIG.INI and BOOTP.TAB configuration files from the Call Server. The Voice Gateway Media Cards are notified to FTP the files from the Call Server.

OTM 2.0's Navigators incorporate links to each CSE 1000 Element Management Web server in a network.

> ***Note:*** For the remainder of this document, CSE 1000 Element Management is referred to as Element Management.

For more information, refer to *Element Management* (553-3023-222).

Enhanced Call Statistics

IP Line 3.0 introduces an additional level of statistics information that can be collected.

LD 32

New LD 32 commands

Four new commands have been added to LD 32. The new commands are:

- ENCT CARDS L S C <customer>
- ECNT ZONE zoneNum <customer>
- ECNT NODE nodeNum
- ECNT SS hostName

Table 11 on page 65 describes these new commands.

Table 11
Additional LD 32 commands (Part 1 of 2)

Command	Description
ECNT CARD L S C <customer>	This command prints the number of Internet Telephones registered for the specified card. • If the <customer> parameter is specified, the count is specific to that customer. A card must be specified to enter a customer. Otherwise, the count is across all customers. • If no parameters are entered, the count is printed for all zones. A partial TN can be entered for the card (L or L S) which then prints the count per that parameter. A customer cannot be specified in this case. Example: ecnt card 81 << Card 81 >> Number of Register Ethersets: 5 Number of Unregistered Ethersets: 27
ECNT ZONE zoneNum <customer>	This command prints the number of Internet Telephones registered for the specified zone. • If <customer> parameter is specified, the count is specific to that customer. A zone must be specified to enter a customer. Otherwise, the count is across all customers. • If no parameters are entered, the count is printed for all zones. Example: ecnt zone 0 0 << Zone 0 Customer 0 >> Number of Register Ethersets: 4 Number of Unregistered Ethersets: 17

Table 11
Additional LD 32 commands (Part 2 of 2)

Command	Description
ECNT NODE nodeNum	This command prints the number of Internet Telephones registered for the specified node. • If the nodeNum parameter is not entered, the count is printed for all nodes. Example: ecnt node 8765 << Zone 8765 >> Number of Register Ethersets: 3
ECNT SS hostName	This command prints the number of Internet Telephones registered for the specified Signaling Server. • If hostName parameter is not entered, the count is printed for all signaling servers. Example: ecnt ss << Signaling Server: BVWAlphaFox IP 10.10.10.242>> Number of Register Ethersets: 1000

Error messages for the new LD 32 commands

Error messages are printed when invalid data is entered for these new commands. The messages include valuable information such as the correct ranges for the command parameters. See the following tables for the error messages:

- Table 12: "ECNT Card command error messages" on page 67.
- Table 13: "ECNT Zone command error messages" on page 67.
- Table 14: "ECNT Node command error messages" on page 68.
- Table 15: "ECNT SS command error message" on page 68.

Table 12
ECNT Card command error messages

Error	Error Message
Slot out of range error	Slot out of range. Range: [61-99]
Slot non-virtual loop error	Slot does not correspond to a virtual loop.
Slot not configured loop error	Slot corresponds to a virtual loop but it is not configured.
Customer out of range error	Customer out of range. Range: [0-31]
Customer not configured error	Customer does not exist.
Combination of invalid slot and invalid customer	Slot does not correspond to a virtual loop. Customer out of range. Range: [0-31]

Table 13
ECNT Zone command error messages

Error	Error Message
Zone out of range error	Zone out of range. Range: [0-255]
Zone not configured error	Zone not configured.
Customer out of range error	Customer out of range. Range: [0-31]
Customer not configured error	Customer does not exist.
Combination of invalid zone and invalid customer error	Zone not configured. Customer out of range. Range: [0-31]

Table 14
ECNT Node command error messages

Error	Error Message
Node out of range error	Node out of range. Range: [0-9999]
Node not configured error	Node not registered.

Table 15
ECNT SS command error message

Error	Error Message
SS not found in system error	Signaling Server <name> does not exist.

LD 2 system traffic report

A new system traffic report 16 in LD 2 is created on the Succession CSE 1000 Rel 2.0 system to add the printing of Internet Telephone data at the zone level. The data is printed for the following categories at the end of each collection period on a per zone basis (the counts are reset after the data is printed):

- Total inter/intra calls made
- Total inter/intra calls blocked
- Percent average inter/intra zone bandwidth used
- Percent maximum inter/intra zone bandwidth used
- Total inter/intra zone bandwidth threshold exceeded count

The "Total inter/intra zone bandwidth threshold exceeded count" prints the number of times a user configured bandwidth threshold was exceeded for the zone during the collection period. The existing LD 2 commands that are related to setting the system threshold are used with a new value defined for the bandwidth threshold.

Table 16
System threshold commands

Command	Description
TTHS TH tv	Prints the current system thresholds.
STHS TH tv -- TV	Sets the system thresholds.
Note 1: The system thresholds TH values 1-4 already exist. A new TH value of 5 is used for the zone bandwidth threshold. ***Note 2:*** The system thresholds TV value is the percentage of the zone's maximum bandwidth. The range values are 000-999, where 000 corresponds to 00.0% and 999 corresponds to 99.9%. The default is 90.0%.	

The following examples first set the system bandwidth to 75% and then prints the actual value.

```
.STHS 5 750
.TTHS 5
```

The system traffic report 16 outputs data in the following format:

zone cmi cmo cbi cbo pi po ai ao vi vo

Table 17 describes the output data.

Table 17
System traffic report 16 data output

Data	Description
zone	Number of the zone
cmi	Intrazone calls made
cmo	Interzone calls made
cbi	Intrazone calls blocked
cbo	Interzone calls blocked
pi	Intrazone peak bandwidth (%)
po	Interzone peak bandwidth (%)
ai	Intrazone average bandwidth usage (%)
ao	Interzone average bandwidth usage (%)
vi	Intrazone threshold violations
vo	Interzone threshold violations

An example of the printout is:

```
.invs 16
0000 TFS016

000 00005 00003 00000 00000 07 03 02 01 000 000
001 00003 00003 00000 00000 03 2 01 01 000 000
```

All other commands (SOPS, COPS, TOPS) function as normal. Table 18 shows the SOPS, COPS, and TOPS commands:

Table 18
SOPS, COPS, TOPS commands

.tops 1 2 3 4 5 14	Displays the current system report list
.sops 1 2 3 4 5 14 -- 16	Add report 16 to be printed
.tops 1 2 3 4 5 14 16	Display system report list with report 16 added
.cops 1 2 3 4 5 14 16 -- 16	Delete report 16
.tops 1 2 3 4 5 14	Display system report list with report 16 deleted

Programmable line (DN) / Feature Key Labels

IP Line 3.0 gives the Internet Telephone user the ability to program the label on the feature key. This label change is saved and then displayed on the feature key. Feature keys are available on the i2002 (four feature keys) and i2004 Internet Telephones (six feature keys) and the i2050 Software Phone.

Prior to IP Line 3.0, a user could program a feature key for calling a certain phone number, for example, their home phone number. The label on the feature would be displayed as the phone number, for instance 555-1234. With the new IP Line 3.0 programmable line (DN) / Feature Key Labels, the user can change the label to say “Home” instead of their home phone number. The label can be up to a maximum of 10 characters.

The Feature Key labels for each Internet Telephone are stored in a text file in the c:/u/db/database.rec directory on the Call Server. The label information is retrieved from the file during the sysload of the Call Server into memory. When the Call Server performs EDD, the information is dumped to the file.

When the telephone registers, the Call Server looks up the Feature Key label in the memory based on the TN of the Internet Telephone. If the labels are found, they are sent to the telephone through SSD messages when the key map download occurs. If the labels are not found, the Call Server sends out the key number strings or key functions.

System impact

The Feature Keys (self-labeled) use space on the Call Server's /C: drive (flash or hard drive) to store its database and needs a structure to hold the information in memory. A system must have enough space in the memory and flash drive to store the database.

This feature introduces new messages into the network. A single SSD message can transfer only two characters. At the key map download time, it needs a maximum 60000 SSD messages from the Call Server to IP Line.

60000 = (5 x 12 x 1000) where:
- 5 SSD messages to send one label
- 12 feature keys (6 keys on 2 feature key pages)
- 1000 Internet Telephones on the Signaling Server

When the user changes the feature key label, SSD messages are sent from IP Line to the Call Server. The Call Server has to save this information to memory and as a result, this information can impact the performance of the Call Server.

For more information about programmable line (DN)/feature keys (self-labeled), refer to *Internet Terminals Description* (553-3001-217).

Private Zone Configuration

DSP resources for each customer are placed in one common pool. A DSP channel is allocated to an IP to circuit-switched call based on a round-robin searching algorithm within the pool.

If an available resource cannot be found, the overflow tone is given. For most installations, this approach works because all Internet Telephone users share the IP Line DSP resources. The DSPs can be provisioned using a DSP-to-Internet Telephone ratio similar to trunk resources since the DSPs are used only for circuit-switched access or conference calls.

When IP to PSTN calls are used, such as with ACD agents or other users who consistently are using trunk resources when making calls, it becomes difficult to provision the system in a way that guarantees an available DSP channel when these users need it.

If the other users suddenly make a lot of conference calls or trunk calls, the DSP resources can deplete and as a result, calls cannot be made. This occurs because all DSP channels are in one pool. To address this situation, the IP Line 3.0 application adds the new Private Zone Configuration feature for DSP configuration and allocation. This new feature enables the configuration of one or more gateway channels as a private resource to guarantee DSP availability for critical or ACD agent Internet Telephones.

A new Private Zone classification has been added to the zone configuration. A zone can now be configured as shared or private.

Shared Zone

The current default zone type is a shared zone. The Internet Telephones configured in shared zones use DSP resources configured in shared zones. If all the shared zones' gateway channels are used, the caller receives an overflow tone and the call is blocked. Select gateway channels in the following order:

- Select a channel from the same zone as the Internet Telephone is configured.
- Select any available channel from the shared zones' channels.

Private Zone

The private zone is the new zone type introduced in IP Line 3.0. DSP channels configured in a private zone are used only by the Internet Telephones that have also been configured for that private zone. If more DSP resources are required by these Internet Telephones than what is available in the zone, DSPs from other shared zones are used.

Internet Telephones configured in shared zones cannot use the private zones' channels.

Select the gateway channels in the following order:

- Select a channel from the same private zone as the Internet Telephone is configured.
- Select any available channel from the pool of shared zones' channels.

LD 117

DSP channels and Internet Telephones are set as shared or private based on zone configuration. A new parameter was added to the zone configuration commands in LD 117. Zone configuration can be set to either shared or private using the parameter <zoneResourceType>.

A zone is configured in LD 117 as follows:

NEW ZONE <zoneNumber> [<intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <newResourceType>]

CHG ZONE <zoneNumber> [<intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <newResourceType>]

By default, a zone is configured as shared (newResourceType=shared).

Example

The command to add a new zone, zone 10, is:

new zone 10

Zone 10 added. Total number of Zone = n
(where n is the total number of zones)

The **prt zone** command is used to see details for all configured zones. See Table 19 for sample output of the prt zone command.

Table 19
Sample output from prt zone command

			Intrazone				Interzone				
Zone	State	Type	Bandwidth (Kbps)	Strategy	Usage (%)	Peak (Kbps)	Bandwidth (Kbps)	Strategy	Usage (%)	Peak (Kbps)	HO/BRCH
0	ENL	SHARED	100000	BQ	0	0	100000	BQ	0	0	HO
1	ENL	SHARED	10000	BQ	0	0	10000	BQ	0	0	HO
4	ENL	PRIVATE	10000	BQ	0	0	10000	BQ	0	0	HO
10	ENL	SHARED	10000	BQ	0	0	10000	BQ	0	0	HO

Function of the shared and private zones

If a resource-critical Internet Telephone is configured for a private zone, and there are not enough resources found within that zone, the search continues to the shared zones within the same customer for an available DSP channel.

However, if a phone is configured in a shared zone, the PBX/Call Server limits its search to the pool of shared DSP channels. That is, the Internet Telephone does not search into the private zones’ channels.

When configuring the allocation of shared versus private resources, consideration must be given to the number of private resources that are needed. Enough DSP resources should be configured to prevent the Internet Telephones configured in shared zones from running out of channels.

WARNING

The PBX/Call Server does not search for channels in private zones if it is configured to use only shared zones. Only Internet Telephones configured in the same private zone can use the private zone voice gateway channels.

Since the channels in the private zone are not accessible to Internet Telephones in the shared zone, ensure that only enough private channels are configured to cover the Internet Telephones in private zone. Do not configure more than is needed in the private zone because the shared zone telephones do not have access to these channels.

Interworking with NAT

Network Address Translation (NAT) provides the following benefits:

- the ability to network multiple sites with overlapping private address ranges
- the added security for servers on a private network
- the conservation of public IP address space

A NAT device exists between a private network and a public network. The NAT device maps private addresses to public addresses.

IP Line 3.0 NAT

IP Line 3.0 does not support all the benefits of NAT listed above. IP Line 3.0 implements only a periodic message feature to keep NAT sessions alive when a call is on mute. The periodic messaging prevents an RTP packet stream NAT session from timing out. This could occur when the Internet Telephone is muted and packet transmission is stopped.

To support multiple Internet Telephones behind one NAT device, it is necessary for NAT to map between public and private IP addresses, and ports for each Internet Telephone behind it. The mapping should include both a signaling port and media (voice) port. In a situation where there are multiple NATs between the Internet Telephone and the Voice Gateway Media Card, all NATs on the path have to follow the rules described in the following sections for signaling and media streams.

Mapping is configured and implemented using the NAT device. The IP Line application does not implement any of the mappings.

NAT and Signaling

NAT hides the true identity of the Internet Telephone from the TPS. The TPS knows only the IP address and port number of the Internet Telephone.

Signaling messages between the Voice Gateway Media Card and Internet Telephones are carried by RUDP. Each RUDP connection is distinguished by its IP address and port number. The NAT does one-to-one mapping on the signaling port for each Internet Telephone behind it to support multiple phones. The TPS uses fixed port numbers for signaling, NAT must do a one-to-one mapping for these port numbers. Table 20 on page 78 lists the UDP port number used.

Table 20
Signaling UDP Ports

UDP Port	Device	Use
5000	Internet Telephone	Incoming signaling messages to the Internet Telephone
5100	TPS	Incoming call processing messages to the TPS
4100	TPS	Incoming registration message to Connect Server
7300	TPS	Incoming registration messages to node Master

NAT and Media Streams

The media stream port numbers on the Voice Gateway Media Card use a fixed numbering scheme where the starting number for the port range is configurable. The first port on the card uses the configured starting port number and subsequent ports are numbered in a monotonically increasing manner. Each port has two sequential numbers: one for RTP and one for RTCP.

> ***Note:*** The NAT has to provide one fixed public port number (5200) for all media streams to and from Internet Telephones behind it.

This port should not be changed at any time, and it should map to port 5200 on the Internet Telephones.

Table 21
IP Line Media Path UDP Ports

UDP Port	Device	Use
5200-5262	Succession Media Card	RTP packets (configurable starting port number - Internet Telephone’s port matches it)
5201-5263	Succession Media Card	RTCP packets into Succession Media Card (port number is RTP port number + 1)
5200-5246	ITG-P Line Card	RTP packets (configurable starting port number - Internet Telephone’s port matches it)
5201-5247	ITG-P Line Card	RTCP packets into SMC (port number is RTP port number + 1)
5200	Internet Telephone	RTP packets into internet phone (port matches first RTP port of the Voice Gateway Media Card)
5201	Internet Telephone	RTCP packets into Internet Telephone (port matches first RTCP port of the Voice Gateway Media Card)

Mute and Hold Considerations

IP Line 3.0 has to handle two special cases when interworking with NAT. These are mute and hold.

Mute

When a user enables Mute, the TPS sends a Mute Transmit (Tx) command to the Internet Telephone. This forces the telephone to generate silence in the transmit direction. If the telephone is using an evocator that implements silence suppression, for example G.729AB, the telephone sends one silence frame to the far end, and then stops sending any further frames until Mute is cancelled. As a result, data sent from the Internet Telephone stops.

The NAT device sees that the Internet Telephones's UDP connection is not active in the transmit direction and starts aging the translation. Depending on the length of time the call is muted and the duration of the NAT's translation aging timeout value, it is possible for the NAT device to timeout the translation and drop the connection. At this point, all packets coming from the far end would be dropped by the NAT device.

At the time mute is cancelled, the Internet Telephone starts transmitting again. NAT considers this to be a new connection and creates a new translation, sending data to the far end using this new translation. This results in half-duplex voice connection between the Internet Telephone and the far end device. In this case, data sent to the far end device gets there; however, the data coming back is lost.

To solve this problem, the Internet Telephone must periodically send an extra non-RTP packet to the far end to keep the NAT translation alive. This "bogus" packet is sent to ensure that the NAT's session timeout does not expire. The non-RTP packet is constructed to fail any RTP validation tests so it is not played out by the far end device (Internet Telephone or gateway channel).

Hold

The Hold function differs from the Mute function. When an Internet Telephone user places a call on Hold, it closes the audio stream in both the Transmit (Tx) and Receive (Rx) directions. To NAT, it is similar to Mute, and the NAT device begins aging the translation. However, this situation does not require a special treatment on the IP Line application or Internet Telephone firmware. When the call is retrieved from Hold, a new set of open audio stream messages are issued by the TPS and new connections are established. As a result, it does not matter if the NAT device has deleted the earlier session.

Table 22 shows supported operations for Internet Telephones behind a NAT device in IP Line 3.0.

Table 22
IP Line NAT Support Strategy

Requirement	Comment
An Internet Telephone behind a NAT device can be registered.	Yes
An Internet Telephone behind NAT can make a call through the Voice Gateway Media Card channels and also to other Internet Telephones that are not behind the NAT device.	Yes
A call can be established between two Internet Telephones on the same private network (behind the same NAT device).	No
If there are multiple DNs configured on an Internet Telephone, all DNs are able to make and receive calls.	Yes
The user must be able to hold, mute, and retrieve calls.	Yes

Note: While not directly associated with NAT support, the i2002/2004 Internet Telephone firmware continues to be downloaded using Trivial File Transfer Protocol (TFTP). UFTP is not supported. TFTP prevents placing Internet Telephones behind firewalls that have the TFTP port blocked for security reasons. An alternative is to upgrade the Internet Telephones firmware to the latest version prior to placing it behind the firewall.

NAT Configuration

The Element Management Web server and OTM 2.0 GUIs have two new prompts to configure the timer function. A checkbox is used to enable or disable the NAT message. When enabled, a configuration box sets the time (in seconds) between messages sent. The default value is 90 seconds. The configured values apply to all Internet Telephones on the node.

Run-time configuration changes

The ITG Line 2.x applications required the ITG-P Line Card to be disabled and then enabled to activate some administrative changes, and in some cases, a card reboot was required for changes to take effect.

IP Line 3.0 improves this functionality by enabling most changes to be made without disabling or rebooting the Voice Gateway Media Cards. After adding configuration information for a new Voice Gateway Media Card and downloading the BOOTP file to the Leader, a new Voice Gateway Media Card can be added to an existing node without rebooting the other cards.

The following exceptions exist for the changing node properties and these changes are not supported by this enhancement:

- A role change requires a reboot to enable the application to reconfigure itself. That is, changing a Leader to Follower or changing Follower to Leader.
- Changing the node IP, subnet masks, or gateway IP addresses requires a reboot of all cards in the node.
- Changing the IP address of a particular card requires a reboot of that card so it can retrieve its new IP address information.

Therefore, IP Line 3.0 supports only run-time changes for the following:

- changes to the CONFIG.INI file
- add card or delete card changes to the BOOTP.TAB file

CONFIG.INI file

The following are automatically reconfigured after the CONFIG.INI file is downloaded from OTM to the card:

- DSCP bits setting
- configuration of ELAN link to Call Server
- loss plan
- SNMP traps
- Routing Table
- firmware download
- codec selection

The reconfiguration of firmware download is done only in the Master card. New firmware files are retrieved from the new file server. The Master card then sends out a broadcast message to the Follower cards indicating the need for a file update.

BOOTP.TAB file

If a card is added or deleted from the node, the BOOTP server is updated using the new BOOTP.TAB file. The new card can retrieve its parameters with the next BOOTP request.

Element Management on Succession CSE 1000 Rel 2.0 generates the CONFIG.INI and BOOTP files and places them on the Call Server. It then notifies the Voice Gateway Media Cards to retrieve these files. The BOOTP server normally runs on the Signaling Server but also runs on any Voice Gateway Media Card acting as the Master.

OTM 2.0 on the Meridian 1 and Succession CSE 1000 Rel 1.1 system downloads the BOOTP.TAB file to the node's Leader card. The file is then distributed from the Leader to the Follower cards in the node.

Configuration changes have an effect only on new calls. Existing calls are not interrupted. However, there are exceptions:

- If the active Call Server ELAN link's configuration data is changed (for example, a changed IP address), then active calls are released.

  If the non-active Call Server is changed (for example, survivable side IP address), then the calls are not affected.

  When the ELAN connections are taken down to implement the configuration change, the Internet Telephones and gateway channels registrations are unregistered on the Call Server. The Call Server releases the calls. When the link is re-established, the TPS synchronizes the call states and releases the active calls. Service is interrupted during this re-establishment period and the following are affected:

  - new Internet Telephones cannot register
  - registered Internet Telephones cannot establish new calls
  - the Voice Gateway Media Card's faceplate displays S009

  Once the ELAN link comes up, the Line Terminal Proxy Server (LTPS) reregisters the telephones with the Call Server and all service is resumed.

- If the codec list is changed, the Voice Gateway Media Card's DSPs may need to be reloaded. For instance, one DSP image contains G.711, FAX, and G.729A/G.729AB. The other DSP image contains G.711, FAX, and G.723.1. If the user has a node configured with the G.729AB codec and the user performs an administrative change to use G.723.1 (or vice versa), the DSPs must be reloaded.

  After the CONFIG.INI file containing the administrative change is downloaded to a Voice Gateway Media Card, the card's DSPs are reloaded as they become idle. For instance, if all DSPs are idle on the card, the new image is loaded to all of them at once. If one or more DSPs have calls active, the DSP is not reloaded until the active calls have released. This can cause some DSPs to be reloaded later than others.

This new functionality is supported by both Element Management and OTM 2.0.

Patching tool

A patch is a piece of code that is inserted or patched into an executable program. The patching tool enables loadware on the ITG-P Line Card and Succession Media Card platforms to be patched or fixed without having to upgrade the card loadware and without service interruption. Patches are stored on the MPLS database.

All patch commands on the ITG-P Line Card, Succession Media Card, and Signaling Server are accessible at the IPL> prompt. These commands are summarized in Table 23 on page 86.

The functionality and syntax is similar to the current Call Server patching tool.

> ***Note:*** The exception is that the parameter string supplied to the command must be enclosed with double quotes. For example, the syntax for the pload command is pload “patch1.p”.

These commands are used to manage patches on the Voice Gateway Media Card. Patches must be downloaded from a workstation to the Voice Gateway Media Card using a modem, an FTP session, or Element Management. Patch files are stored in Flash memory and are loaded into DRAM memory. Once a patch is in DRAM memory it can be activated, deactivated, and its status can be monitored.

The technician must perform the following tasks prior to loading a patch:

- Check that the patch matches the platform’s CPU type.
- Check the loadware version on the card.
- Block the installation if there is a mismatch.

The installation of a patch is blocked if either the CPU type or the loadware version of the card is different than the patch. If the installation is blocked, the reason for blocking the install is printed at the CLI. The CPU type and loadware version are also checked during a power-up or reboot cycle. This prevents active patches from being re-installed if the loadware version of the card is changed.

Table 23 on page 86 lists the patch commands.

Table 23
Patch commands (Part 1 of 3)

Command	Description
pload	Loads a patch file from the file system in Flash memory into DRAM memory. The loaded patch is inactive until it is put into service using the pins command. When a patch is successfully loaded, the pload command returns a **patch handle number**. The patch handle number is used as input to other patch commands (pins, poos, pout, and plis). Syntax: pload "[patch-filename]" where [patch-filename] is the filename or path of the patch file. If a filename alone is provided, the patch must be in the /C:/u/patch directory. Otherwise, the full or relative path can be provided. If the pload command is issued without a parameter, the technician is prompted for the patch filename and other information.
pins	Puts a patch that has been loaded into memory (using the pload command) into service. This command activates a patch. If issued successfully, the pins command indicates that global procedures, functions, or areas of memory are affected by the patch. The technician is then prompted and has the choice to proceed or not to proceed. Syntax: pins "[handle]" where [handle] is the number returned by the pload command If the pins command is issued without a parameter, the technician is prompted to enter a handle.

Table 23
Patch commands (Part 2 of 3)

Command	Description
poos	Deactivates a patch (takes it out-of-service) by restoring the patched procedure to its original state. Syntax: poos "[handle]" If the poos command is issued without a parameter, the technician is prompted to enter a handle.
pout	Removes a patch from DRAM memory. The patch must be taken out-of-service (using the poos command) before it can be removed from the system. Syntax: pout "[handle]" If the pout command is issued without a parameter, the technician is prompted to enter a handle.
pstat	Gives summary status information for one or all loaded patches. For each patch, the following information is displayed: patch handle, filename, reference number, whether the patch is in-service or out-of-service, the reason why the patch is out-of-service (if applicable), and whether the patch is marked for retention or not. ***Note:*** Patch retention means that if a reset occurs, then the patch is automatically reloaded into memory and its state (active or inactive) is restored to what it was prior to the system going down. Syntax: pstat "[handle]" If the handle is provided, only the information for the specified patch is displayed. If the pstat is issued without a parameter, information for all the patches is displayed.

Table 23
Patch commands (Part 3 of 3)

Command	Description
plis	Gives detailed patch status information for a loaded patch. Syntax: plis “[handle]” If the pout command is issued without a parameter, the technician is prompted to enter a handle.
pnew	Creates memory patches for the Voice Gateway Media Card. • The release of the patch is assumed to be the same as that of the current load. • The address to be patched is checked to ensure that it is in range. • For each address that is changed, the “old” contents are assumed to be the current contents of that memory address. • If a path is not provided for the new path filename then it is assumed that the patch is in the /C:/u/patch directory. Once a memory patch is created using the pnew command, it is loaded and activated like any other patch. Syntax: pnew ***Note:*** The pnew command has no parameter(s).

Patch Directories

There are two patch directories on a Voice Gateway Media Card:

1 **/C:/u/patch**

This is the default directory for patch files. Patch files should be copied to this directory.

2 **/C:/u/patch/reten**

The technician uses this directory to store patch retention control files. Do not use this directory to store patches and do not remove files from this directory.

Patch Synchronization Across a Node

The Succession CSE 1000 Rel 2 Element Management Web server provides a mechanism for downloading and putting patches in service across a node.

Patch synchronization across a node cannot be carried out from the IPL> prompt. On Meridian 1 or Succession CSE 100 Rel 1 systems, patch synchronization is a manual operation that must be performed at the CLI of each Voice Gateway Media Card.

Virtual Office

Succession CSE 1000 Rel 2.0 and IP Line 3.0 provides the Virtual Office feature. This feature enables a user to use any Internet Telephone within the network.

The Virtual Office feature provides a call service to "travelling" users who want to use a different physical Internet Telephone (other than the telephone they normally use). Users can login to another Internet Telephone using their DN and pre-configured Station Control Password (SCPW).

Once logged in, users have access to their DNs, autodial numbers, key layout, feature keys, and voice mail indication/access that are configured on their own home-office Internet Telephones. For example, if users go to another office or to a different location within the same office, they can login to any available Internet Telephone and have all the features of their home-office Internet Telephone. When the user logs off the Internet Telephone, the features that were "transferred" to that telephone are removed.

Virtual Office is supported for the i2002 and i2004 Internet Telephones, and the i2050 Software Phone. An i2004 or i2050 user is prevented from accessing this feature from an i2002 Internet Telephone. Table 24 on page 90 shows which user can log in to particular telephones.

Table 24
Virtual Office login from various telephones

Internet Telephone User	Virtual Office login
An i2002 Internet Telephone user...	...can Virtual Office login from i2002, i2004, and i2050.
An i2004 Internet Telephone user...	...can Virtual Office login from i2004 and i2050. ...receives a "Permission Denied" message when the user attempts a Virtual Office login from an i2002 Internet Telephone.
An i2050 Software Phone user...	...can virtually login from i2004 and i2050. ...receives a "Permission Denied" message when the user attempts a Virtual Office login from an i2002 Internet Telephone.

Virtual Office User Allowed (VOUA) and Virtual Office Login Allowed (VOLA) must be configured on the Internet Telephones as follows:

- The Internet Telephone where the user wants to virtually login (destination) must have Virtual Office User Allowed (VOUA) configured.
- The Internet Telephone where the user wants to login from (source) must have Virtual Office Login Allowed (VOLA) configured.

  Note: Three failed password attempts to login using the Virtual Office feature locks the user out from Virtual Office login at the Call Server for one hour. The Call Server lock can be removed by an administrator using an LD 32 command to disable and re-enable that TN. Refer to *Maintenance* (553-3023-510) for more information.

An Internet Telephone registers using the TN (in its EEPROM), and then a valid user id and password are used to determine the Home TPS for the Internet Telephone during the Virtual Office connection. A Succession CSE 1000 Gatekeeper is required if the Home TPS is not the TPS where the Internet Telephone is registered when the Virtual Office login is initiated.

Virtual Offices provides the following capabilities:

1 A network-wide connection server (Gatekeeper) is equipped to provide addressing information of call servers, based on a user's DN.

2 The user can enter a key sequence at an Internet Telephone to initiate the login sequence. The user enters their current network DN and a user-level password. The password is the Station Control Password configured in LD 11. If a SCPW is not configured, the virtual office feature is blocked.

3 A user logs out when leaving the location.

For more detailed information about Virtual Office, see *Internet Terminals Description* (553-3001-217).

Branch Office

The Succession Communication Server for Enterprise (CSE) 1000 Branch Office provides a means of extending Succession CSE 1000 features to one or more remotely-located Branch Offices.

The Succession CSE 1000 Branch Office is a feature set of the equipment and software that a secondary location needs to centralize the call processing of its IP-based communications network. The Call Server at the Main Office provides the call processing for the Internet Telephones in both the Main Office and Branch Offices. The H.323 WAN Gateway in the Branch Office provides access to the local Public Switched Telephone Network (PSTN).

The Succession CSE 1000 Branch Office is connected to the Main Office over a virtual trunk on a WAN. Internet Telephone calls and IP network connections are controlled by, and come from, the Main Office. If the Main Office fails to function, or if there is a network outage, the Succession System Controller (SSC) at the Branch Office provides service to the telephones located in the Branch. The telephones then survive an outage between the Branch Office and the Main Office.

The basic hardware of a Branch Office includes the H.323 WAN Gateway and the Signaling Server. The H.323 WAN Gateway provides access to the local PSTN for users in the Branch. It also provides support for analog devices such as fax machines or telephones in the Branch Office.

For detailed information about Branch Office, refer to *Branch Office* (553-3023-221).

802.1Q Support

Firmware version 1.3x of the i2002/2004 Internet Telephone enables 802.1Q support. 802.1Q support enables the definition of virtual LANs (VLANs) within a single LAN. This improves bandwidth management and limits the impact of broadcast and multicast messages.

Supporting 802.1Q on the Internet Telephones enables VLAN configuration and packet prioritization to be simplified. These are configured at the Internet Telephone instead of at the network switch port for each telephone. The “p” bits within the 802.1Q standard enable packet prioritization at Layer 2 and this improves network throughput for VoIP data. The network switching equipment must still be capable of recognizing and processing the 802.1Q header. However, 802.1Q support reduces the configuration necessary to add VLAN and prioritization functionality.

Only the i2002 and i2004 Internet Telephones generate the 802.1Q header. The ITG-P Line Cards and Succession Media Cards do not. As a result, the switch ports for the Voice Gateway Media Card TLAN ports must be configured as untagged ports so the header is removed.

VLAN ID and Priority Field

The 802.1Q VLAN ID:

- Provides a higher level of security between segments of internal networks.
- Breaks large networks into smaller parts to prevent consumption of bandwidth to broadcast and multicast traffic.

The 802.1Q Priority field enables classification of UDP traffic for prioritization through network Layer 2 switching.

802.1Q Tag

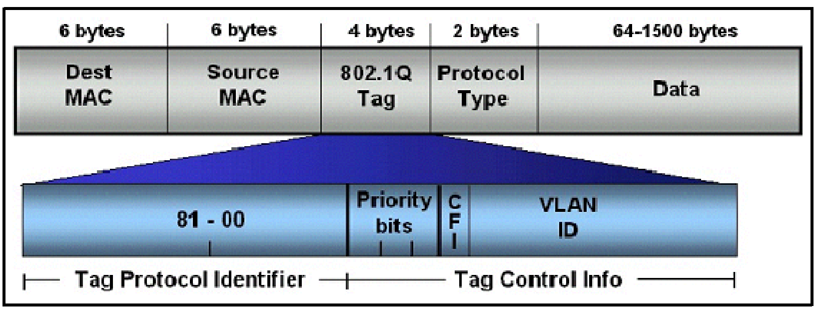
A standard Ethernet frame contains a header consisting of a 6-byte destination MAC address, a 6-byte source MAC address, and a 2-byte protocol identifier. Following the header is a data area.

The 802.1Q standard specifies a new format of Ethernet frame. The 802.1Q protocol standard makes extensions to the Ethernet frame by adding four additional bytes to the Ethernet header. One of the four 802.1Q extension fields applies to QoS. This field is a 3-bit priority field that is referred to as 802.1p. These priority bits are shown in Figure 5 on page 94.

The 802.1Q formatted frame is identical to a standard Ethernet frame, with the exception of the 4-byte 802.1Q tag that is inserted between the source MAC address and the protocol identifier. The first 16 bits of the 802.1Q tag field is the Tag Protocol Identifier containing 8100 (hex) (the 802.3 tag format), enabling the Ethernet interface to distinguish it from standard Ethernet frames. The last 16 bits of the 802.1Q tag contain the following information:

- a 3-bit Priority field (the 802.1p bits)
  This field represents the user priority level (7 is the highest).
- a 1-bit Canonical Field Identifier (CFI)
  This field is always set to 0.
- a 12-bit VLAN ID field

Figure 5
802.1Q Tag Format



Automatic VLAN ID Configuration

As part of the 802.1Q feature, an option to automatically discover the VLAN ID using DHCP exists. This process greatly reduces the configuration steps since manually entering the VLAN ID data is not required.

When automatic VLAN discovery using DHCP is used to obtain the VLAN ID and the Internet Telephone is configured using DHCP, the following occurs automatically:

- The i2002 and i2004 Internet Telephones perform an initial DHCP Discovery Request in the default VLAN.
- The DHCP server returns a DHCP ACK message with an IP address in the data VLAN and one or more voice VLAN IDs in the vendor-specific field (refer to Appendix G on page 719 for an example of the DHCP configuration strings).
- The Internet Telephone reads the voice VLAN ID(s) and saves them.
- The Internet Telephone rejects the DCHP offer (accepts it but immediately gives up the lease).
- The Internet Telephone reboots and sends a DHCP Discovery Request with the first VLAN ID from the saved list. This is repeated for each VLAN ID in the list until a response is received.

  This works because the Layer 2 switch discards every DHCP Discovery Request it receives from the Internet Telephone if the VLAN ID does not match the VLAN IDs configured on the port. When the Internet Telephone sends a DHCP Discovery Request with the port's configured VLAN ID, the packet passes into the network and the DHCP server's ACK message is passed back.

- When a DHCP ACK message is received, the Internet Telephone accepts the offer and saves the IP address, Node IP address, and other IP parameters.

The Internet Telephone's use of 802.1Q

The i2002/i2004 Internet Telephone supports 802.1Q as follows:

- 802.1Q can be enabled or disabled at boot time using manual configuration or control downloaded from the TPS.
  - If 802.1Q is disabled, standard Ethernet frames are transmitted.
  - If 802.1Q is enabled, all frames transmitted by the Ethernet driver have the 802.1Q tag bytes inserted between the source MAC address and the protocol type field. The tag protocol identifier field contains 8100 (hex) and the CFI bit set to 0.
- By default, when 802.1Q is enabled, the priority bits of all frames are set to 6 (octal) and the VLAN ID is set to 000 (hex). The GUI and TPS configured values override these values.
- The Internet Telephone's Ethernet driver receives any Ethernet frame destined for it, regardless of whether 802.1Q is enabled or whether the received frame is an 802.1Q tagged frame. The only exception is any 802.1Q tagged frame with the CFI=1. In this case, the frame is discarded.
- The Internet Telephone's Ethernet driver strips the 802.1Q tag information from the frame prior to passing it on to the IP stack. Priority and VLAN information on received frames are not preserved and are ignored.

Configuration of the Internet Telephone's 802.1Q

The 802.1Q support for the Internet Telephones is configured and controlled using the telephone's user interface or DHCP. The DHCP approach eliminates the need to manually set the VLAN ID during the installation. To configure 802.1Q, set the following: "p" bits and VLAN ID.

Setting the "p" bits

By default, the 3-bit field "p" bits are set to 110b (6), which is the value recommended by Nortel Networks. The "p" bit value can be changed using either OTM or Element Management. The same "p" bit values are assigned to the RTP media stream and the UNIStim control signaling stream. The TPS sends the "p" bit value to the telephone using a UNIStim messaging.

There are two fields in the OTM and Element Management GUI used to set the “p” bits:

1 A **checkbox** that, when checked, means the priority bits should be set to the value specified by the 802.1Q priority bit value field. If the checkbox is unchecked, the i2002/i2004 Internet Telephone sends out the default priority of 6.

2 A **802.1Q priority bit value field**. This field sets the value that the i2002/i2004 Internet Telephones sends out. The range is 0-7.

Setting the VLAN ID

The contents of the VLAN ID field can be specified on a "per interface" basis. There is only one network interface on the i2002 and i2004 Internet Telephones, therefore, the setting of the VLAN ID field is a "global" setting. That is, all packets transmitted by the Internet Telephone have the same VLAN ID.

The VLAN ID is specified as follows:

- the default VLAN ID is 000 (hex)
- the VLAN ID can be set during a manual configuration of the Internet Telephone using the telephone keypad, or automatically retrieved using DHCP (automatic VLAN discovery).

  Note: For more information about manual or automatic Internet Telephone configuration, refer to *Internet Terminals Description* (553-3001-217).

Some implementation requirements of the Automatic VLAN Discovery using DHCP are:

1 A DHCP server IP address pool must exist for each subnet (also VLANs). This is standard DHCP operation. The requirement would be the same for PCs or Internet Telephones.

2 A DHCP server should not exist in more than one VLAN at one time (one subnet for each VLAN), unless the link to the DHCP server is tagged and the DHCP server can recognize this. With an untagged link to the DHCP server, traffic could originate on one VLAN and end up on the other VLAN. In this case, the VLAN using DHCP feature does not work.

3. Voice and data subnets must be separate if the three-port switch with VLANs is being used.
4. A layer three switch (or router) with a Relay agent must be used because traffic from the voice VLAN to the data VLAN must be routed. Presumably, the DHCP server is on the data VLAN. Without a Relay agent a DHCP server must exist on each subnet.
5. At least two IP address pools are used on the DHCP server. One for the Voice VLAN/subnet and another for the Data VLAN/subnet. Additional pools can be added as required as long as one IP address pool per subnet and VLAN is used. A relay agent is required if it is a PC-only network.

Control of the Internet Telephone's 802.1Q

The 802.1Q header in the outgoing packets from the i2002 and i2004 Internet Telephones is enabled by one of the following:

- If the Internet Telephone's VLAN GUI response is set to 1, then the 802.1Q functionality is enabled. All packets from the Internet Telephone have the 802.1Q header as part of the Ethernet frame.
- If the Internet Telephone's VLAN GUI response is set to 2, then the 802.1Q functionality is enabled after the DHCP response is received with the VLAN ID.
- If the OTM/Web server configuration enables the use of the "p" bits, once downloaded to the Internet Telephone, the 802.1Q functionality is enabled.

Table 25 on page 99 shows the relationship between the data configured at the TPS and the Internet Telephone (using the GUI or DHCP discovery) and the resulting 802.1Q data sent.

Table 25
Relationship between TPS and GUI configuration to 802.1Q

<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="2">Phone 802.1Q setting
(by GUI or DHCP)</th></tr>
<tr><th>Disabled</th><th>Enabled
VLAN ID = nnn</th></tr>
<tr><th rowspan="2">OTM / Element Management
802.1p Setting</th><th>Disabled</th><td>Normal Internet Telephone Frames</td><td>802.1Q Tagged Frames
Priority = 6
CFI = 0
VLAN ID = nnn</td></tr>
<tr><th>Enabled;
Priority = P</th><td>802.1p Priority Tagged Frames
Priority = P
CFI = 0
VLAN ID = 000</td><td>802.1Q Tagged Frames
Priority = P
CFI = 0
VLAN ID = nnn</td></tr>
</table>

802.1Q and the Voice Gateway Media Cards

The ITG-P Line Card and Succession Media Card cannot send the 802.1Q header because the cards' operating system does not support it. The switch ports connected to the ITG-P Line Card's or Succession Media Card's TLAN should be configured for untagged operation so if a 802.1Q header is present it is stripped before a packet is passed to the card.

The configuration in OTM and Element Management is for the control of the priority bits in the 802.1Q header sent by the Internet Telephones only.

Data Path Capture tool

IP Line 3.0 contains the Data Path Capture tool. A built-in utility used to capture audio information. This tool can help debug audio-related gateway problems and allows after-the-fact analysis of what the user heard.

The audio data captured using the Data Path Capture tool is saved in DRAM in either a circular or a fixed-duration buffer.

- A circular buffer functions in such as way that when the end of the buffer is reached, the new audio data overwrites data at the beginning of the buffer. As a result, a circular buffer always has the most current data contained in the buffer.
- A fixed-duration buffer captures data until the buffer is full. When the buffer is full, the capture process stops.

Once the data is captured, it can be saved to a device on the LAN (using FTP) or it can be written to the flash memory card in the PC Card slot on the Voice Gateway Media Card.

The Data Path Capture process is controlled by a set of CLI commands.

i2002 and i2004 Internet Telephone Firmware

New Firmware, version 1.38 minimum

Version 1.38 of the i2004 and i2002 Internet Telephone firmware (F/W) is the minimum version that is supported with IP Line 3.0. This firmware version contains the following changes:

- upgrades the pSOS+ operating system from a special version to the normal release version.
- enables the support of Virtual Office / Branch Office
- the new operating system version enables the support of 802.1Q (see "802.1Q Support" on page 93).

Firmware Download

In ITG Line 2.0-2.2, the i2004's firmware file was downloaded from OTM to each of the Voice Gateway Media Cards and saved in a directory on the card's Flash disk. As each i2004 Internet Telephone registered, the TPS determined if a firmware upgrade was required and directed the i2004 Internet Telephone (requiring the upgrade) to the FTP server of the card.

The introduction of the i2002 Internet Telephone in IP Line 3.0 requires changes to the way the firmware file is handled.

When the firmware file is downloaded from OTM, it is compressed as it is stored on the /C: drive. File compression reduces the firmware file to less than 900 K. However, the /C: drive Flash disk space is limited on the ITG-P Line Card.

The Internet Telephones may not be distributed with the correct version of the F/W file pre-loaded except in cases where the TFTP download to the Internet Telephone is blocked. For example, if the Internet Telephone is located behind a firewall.

The Internet Telephone normally does not have to be pre-loaded with the firmware file because, during normal operation, the Internet Telephone's firmware is automatically upgraded as part of the registration to the TPS. If the firmware cannot be upgraded because of firewall restrictions, then the Internet Telephone must be upgraded with the current firmware version before distributing the telephone.

Firmware filenames

The Internet Telephone firmware files are released on CD-ROM. The files are also available from the Nortel Networks Web site (see Appendix G: "Downloading IP Line files from Nortel Networks Web Site" on page 719).

The Internet Telephone firmware files are labelled as follows:

- 0602Bnn.BIN is the filename for the i2004 Internet Telephone firmware where Bnn = F/W version 1.nn.
- 0603Bnn.BIN is the filename for the i2002 Internet Telephone firmware where Bnn = F/W version 1.nn.

If the external file server option is used (in OTM or Element Management) for firmware distribution with a node, the files must be renamed before being placed on the server:

- 0602Bnn.BIN must be renamed to i2004.fw
- 0603Bnn.BIN must be renamed to i2002.fw

For the external file server options:

- see Procedure 22 on page 297 for OTM
- see Procedure 39 on page 359 for Element Management

Meridian 1 and Succession CSE 1000 Rel 1

Default location of firmware files

The firmware file for the i2004 Internet Telephone is stored in the C:/FW directory. This is the same directory that is used in the IP Line2.0-2.2 products. The firmware file is downloaded and saved to this directory when the user checks the firmware download checkbox in the OTM Synchronize/Transmit dialog and presses the Transmit button. The IP Line application saves the file i2004.fw as fwfile.1 or fwfile.2 for backwards compatibility. The filename is chosen such that the oldest of the two files on the card is overwritten. Then at card bootup time, if the firmware file is not retrieved from the external server or the /A: drive, the /C:/FW directory is accessed and either the fwfile.1 or fwfile.2 is uncompressed. The newer of the fwfile.1 or the fwfile.2 is uncompressed.

Firmware file management with IP Line 3.0

The IP Line 3.0 operates the same as the IP Line2.0- 2.2 product. The firmware file is stored and retrieved from the local /C:/FW directory.

The IP Line 3.0 application searches for the firmware first at the file server, then in the /A:/FW directory, and finally in the /C:/FW directory.

- Normally the file server is not configured in OTM 2.0. OTM 2.0 places IP address 0.0.0.0 in the CONFIG.INI file for the file server address. If an address of "0.0.0.0" (the default) is read from the file, the IP Line 3.0 application ignores the file server settings. As a result, the normal search ends with the firmware file being retrieved from the /C:/FW directory.
- If a file server address is configured, the IP Line 3.0 application operates as described for the Succession CSE 1000 Rel 2.0 system. The file is downloaded into the /ums directory in memory. In order for all of the cards to get the same firmware files, the technician must ensure that the configured file server is up and running before any of the cards boot up.

The "/A:" drive (faceplate PC Card slot) of the Voice Gateway Media Card can also be used with a PC Card containing the firmware files. The card is specified as the server and the file directory specifies the "/A:/FW" drive.

Download Protocol

The TFTP download mechanism is used in IP Line 3.0. The Master card notifies the Followers about changes to the status of the firmware file using a broadcast on the TLAN interface.

> ***Note:*** UFTP is not supported.

Bootup Scenarios

If the Master is unable to retrieve a firmware file, the upgrade policy is set as “Never”. When the upgrade policy is set to “Never”, the Internet Telephone’s firmware version is not checked and the telephone registers with the firmware version that is currently on the telephone.

If the Master card reboots, the Election process selects another Voice Gateway Media Card as the Master. That Voice Gateway Media Card has all firmware files in its memory. When the original Master card finishes rebooting, it becomes the Master and does the normal Master startup procedure for retrieving the firmware files.

In a power-on situation, where all cards reboot together, the first card that is elected Master retrieves the firmware files from the server.

Succession CSE 1000 Rel 2.0

Default location of firmware files

For Succession CSE 1000 Release 2.0 Normal configuration, the default storage location for the firmware files is on the Signaling Server in the /u/fw directory. The firmware file is downloaded to this directory when the user selects the file in Element Management and presses the Transmit button.

Firmware file management with IP Line 3.0

Due to the limited flash drive space on the Voice Gateway Media Cards, a new mechanism for managing the Internet Telephone firmware files is required. IP Line 3.0 manages the firmware file in the following manner:

1 There is one firmware file for each telephone type. These files are saved and retrieved in one of the following two locations:

- **a** to/from a file server
  (The file server can be a dedicated external server, the Call Server, or a Voice Gateway Media Card.)
- **b** to/from a Master card's RAM device

2 The server's information is configured in Element Management and the information is saved in the CONFIG.INI file. The server's IP address, routing table, file path, user name, and password are specified during configuration time.

3 When the Master card boots, it searches for the firmware files on the specified server.

- **a** If found, they are retrieved and stored on the RAM drive in the /ums directory.
- **b** Otherwise,
  - **i.** for a Voice Gateway Media Card, the Master card continues to search for the firmware files in the local A:/fw directory and then the C:/fw directory until the files are found.
  - **ii.** for a Signaling Server, the Master card attempts to search for the firmware files in the /u/fw directory, and then the /A:/fw directory.

The firmware retrieval process is much faster using IP Line 3.0, as the file is written to the RAM drive. ITG Line 2.0-2.2 required more time because the files are written to the Flash drive.

4 When a Follower card boots, it looks for the firmware files on the Master card's RAM drive in the /ums directory.

If the Master has not yet retrieved the files, the Follower waits until the Master sends notification that the firmware files are retrieved. Using FTP, the Follower transfers the files from the Master and stores them in the /ums directory on its RAM drive.

5 Once a firmware file is found and stored in the card's RAM drive, the upgrade manager parses the file and updates its policy based on the firmware version it received from file.

6 Both the i2002 and i2004 Internet Telephones are checked against the upgrade policy at the time they register. If a firmware update is required, the firmware is downloaded from the Signaling Server or the Voice Gateway Media Card's TFTP server to the Internet Telephone.

The firmware file for the i2004 Internet Telephone is saved as i2004.fw and is saved as i2002.fw for the i2002 Internet Telephone. These filenames are required for the upgrade manager to find certain files in either the standalone file server or the Master card's RAM drive.

In order for all Voice Gateway Media Cards to obtain the same firmware files, the technician must ensure that the configured file server is running before any of the Voice Gateway Media Cards boot up.

In Succession CSE 1000 Release 2.0, the Signaling Server acts as the file server and the Master function is on the Signaling Server. As a result, the time to download the firmware files from the file server to the Master is eliminated.

The /A: drive (the PC Card slot on the card's faceplate) of the Voice Gateway Media Card can also be used with a PC Card containing the firmware files; the Voice Gateway Media Card is specified as the server and the file directory specifies the /A: drive.

Graceful Disable

The DISI command in LD 32 can be used to disable the Voice Gateway Media Card's gateway channels when they become idle. This command removes gateway call traffic from a Voice Gateway Media Card, however, it does not remove the Internet Telephones registered to the Voice Gateway Media Card. Therefore, even after the gateway channels are disabled, all telephones registered to the card are impacted when the card is unplugged or reset. Also, if a Voice Gateway Media Card or Signaling Server is the node Master when it is removed, the Internet Telephone registration service is interrupted until the next election occurs.

This Graceful TPS enhancement provides a card level CLI command that disables the LTPS service on the Voice Gateway Media Card or Signaling Server.

The Graceful TPS command:

- prevents new Internet Telephones from registering
- soft resets any idle, registered Internet Telephones

Since the LTPS does not accept new registrations, the Internet Telephones register with another card's LTPS after the reset. Eventually, all Internet Telephones are registered with other LTPSs and the card can be removed without impact to any users.

In addition, if the "to-be-out-of-service" Voice Gateway Media Card is the node Master, an election is held immediately when the LTPS service is disabled to transfer the mastership to another card. On the Signaling Server this is not done, as it would interfere with the Virtual Trunk's redundancy feature that depends on the node mastership. The LTPS is still disabled on the Signaling Server so all Internet Telephones are moved to another TPS. However, if the Signaling Server is the node Master, the mastership remains.

Operation of the TPS DISI

The Graceful TPS Disable is controlled from the CLI of the card. When the disiTPS command is executed on the card's TPS, the following occurs:

- The card does not accept any new registration requests.
- The card soft resets all registered Internet Telephones that are in the idle state and redirects the telephones to the node Master.
- The card soft resets the remaining busy registered Internet Telephones after they release their active call.
- If the card is node Master, an election is held to transfer the mastership. This occurs only on the Voice Gateway Media Card. The Signaling Server's node mastership is not transferred.

Feature Operation of the Voice Gateway DISI

The Voice Gateway can also be disabled from the CLI of a Voice Gateway Media Card. When the disiVGW command is executed, the following happens on that card's Voice Gateway:

- Idle gateway channels are unregistered.
- A busy gateway channel is unregistered when it becomes idle.

  Note: Care should be taken with this command to avoid a problem that can occur when calls are placed on hold. When a telephone has a call on hold, the voice gateway channel on the card is idle; however, it is still reserved in the Call Server. If the Voice Gateway is still disabled when the call is taken off hold, the call does not have a speech path. It is recommended that the LD 32 DISI command is used for disabling the gateway channels.

Graceful TPS CLI Commands

The following Graceful TPS CLI commands are added to the IP Line shell:

Table 26
Graceful TPS commands (Part 1 of 2)

Command	Description
disiTPS	Disables the LTPS service only. No new Internet Telephones are registered on the card and all registered telephones are reset when they become idle. This command applies to both the Voice Gateway Media Card and Signaling Server. On the Signaling Server, this command affects only the LTPS. It does not affect the virtual trunks or gatekeeper components, which means the node mastership is not moved to another TPS.
disiVGW	Disables the Voice Gateway only. All Voice Gateways unregister with the Call Server when they become idle. This command is applicable only to the Voice Gateway Media Card or the standalone IP Line application.
disiAll	Disables both the LTPS service and the Voice Gateway channels. This command is a combination of both disiTPS and disiVGW commands. On the Signaling Server, this command affects only the LTPS. It does not affect the virtual trunks or gatekeeper components, which means the node mastership is not moved to another TPS.

Table 26
Graceful TPS commands (Part 2 of 2)

Command	Description
enaTPS	Enables the LTPS service. This command is used after the disTPS command to bring the LTPS back into service. This command applies to both Voice Gateway Media Cards and the Signaling Server. On the Signaling Server, this command affects the LTPS only. It does not affect the virtual trunks or gatekeeper components.
enaVGW	Enables the Voice Gateway. All gateway channels register with the Call Server. This command is applicable only to the Voice Gateway Media Card or the standalone IP Line application.
enaAll	Enables both the LTPS service and the Voice Gateway channels. This command is a combination of both enaTPS and enaVGW commands. On the Signaling Server, this command affects only the LTPS. It does not affect the virtual trunks or gatekeeper components.

Maintenance Audit enhancement

The ITG Line 2.2 product on the ITG-P Line Card introduced a background audit that watched for tasks that go into a suspended state. Under normal operation, a task should not go into suspended state. However, if it occurs, the card's processing is affected.

ITG Line 2.2 Operation

With the ITG Line 2.2 application, if the audit task finds a suspended task, it performs the following:

- outputs a stack and register dump to the debug port
- outputs a file on the /C: drive
- resets the card

This function provides an automatic way to return the card to service and provides critical debug information. The information is output to the EXCPLOG.n files (where n is a number from 0-3) that are located in the /C:/LOG directory. The new information is placed in these files where it cannot be overwritten by the usual information output to the SYSLOG file when the card reboots.

The auditRebootSet command was the single maintenance audit CLI command that was provided with ITG Line 2.2. The auditRebootSet command disabled the card reboot if any task was found in a suspended state.

IP Line 3.0 Enhancement

This audit feature is enhanced in IP Line 3.0. This new enhancement differentiates between tasks that are critical and non-critical.

- A critical task is any task that the IP Line application needs to function. When a critical task is not functioning properly, it causes noticeable degradation in the IP Line application.
- A non-critical task is any other task that does not cause noticeable degradation to the IP Line application.

If a critical task is found suspended, the stack and register information is dumped and the card is then reset. If a task on the critical task list disappears, it is treated as a suspended task. Therefore, a missing critical task triggers a reboot and a missing non-critical task does not trigger a reboot.

If a non-critical task is found suspended, the information is dumped but the card is not reset. The card is reset when the Voice Gateway Media Card clock reaches 2:00 AM (default reset time). The reset time is configurable from the CLI. This eliminates card resets that impact service for non-critical tasks by delaying them to a non-service impacting time.

Additional CLI commands have been added enabling any task to be marked as critical or non-critical, regardless of its default designation. This could be used, for example, to mark a “misbehaving” task as non-critical to avoid a card reset. This would enable the problem to be debugged.

The Maintenance Task Audit is available only for the IP Line 3.0 application running on the ITG-P Line Card and Succession Media Card. It is not available on the Signaling Server as it does not have the exception handler, stack dump, and syslog file functions of the other cards.

Critical Task List

All application tasks default to the critical task list. These applications include: TPS, VTM, SET, VTILIB, UMS, UMC, RDP, VGW, RTP, RTCP, ELC, baseMMintTask, and A07.

The following VxWorks system tasks are also on the critical task list: tShell, tNetTask, tExcTask, and tTelnetd.

All other tasks are on the non-critical task list. The monitor task is called tMonTask.

Any data entered at the CLI that deviates the operation from the default is saved in the /C:/CONFIG/AUDIT.INI text file. The contents of the file are loaded as the application boots up and provides the required non-volatile storage for entered settings. It is applicable only to the card on which it resides. It can be manually copied from one card to all other cards in the node if desired.

History File

A history file is created when the card starts. The text file is called audit.his and it is stored in the /C:/LOG directory. This file contains a list of the problems found and the actions taken by the maintenance audit. The audit.his file has a fixed size of 4096 bytes.

The most recent records in the file overwrite the oldest records with newer events appear at the beginning of the file. A record in the file is a one-line string with maximum size of 256 characters.

The format for the records in the history file is:

index : (timeString) TMxx taskName: DescriptionString

where:

- index – monotonically increasing record count; wraps after 9999 events
- (timeString) – the time the event was detected
- TMxx – record type: 0-reboot, 1-Suspend, and 2-TaskDisappear
- taskName – the name of problematic task
- DescriptionString – a description of the action taken

An example of the output follows.

IPL> auditHistoryShow

0001 :(APR 25 12:26:25) TM01 tCSV:Suspend

0002 :(APR 25 12:26:50) TM01 tSET:Suspend

0003 :(APR 25 12:26:50) TM00 tExcTask:Reboot

0004 :(APR 25 12:35:55) TM02 tELC:Disappear

0005 :(APR 25 12:35:55) TM00 tELC:Reboot

0006 :(APR 25 12:48:27) TM01 tUMC:Suspend

0007 :(APR 25 12:48:27) TM00 tExcTask:Reboot

0008 :(APR 25 13:15:56) TM01 tUMC:Suspend

0009 :(APR 25 13:15:56) TM00 tExcTask:Reboot

0010 :(APR 25 13:29:35) TM01 tLogTask:Suspend

0011 :(APR 25 13:45:35) TM01 tLogTask:Suspend

The Maintenance Audit CLI commands

There are five CLI commands that support the maintenance audit function as outlined in Table 27.

Table 27
Maintenance Audit commands (Part 1 of 2)

Command	Description
auditShow	Displays the following information: • whether a card reboot is enabled • the time a card reboot will occur if a non-critical task is found suspended • a list of all tasks being monitored and their designation (critical or non-critical) Example: **IPL> auditShow** **Reboot when detect a suspended task --- Disabled** **Critical Task: tTPS tVTM tSET tVTI tUMS tUMC tRDP tPBX tVGW tRTP tRTCP tELC baseMMintTask tA07 tShell tNetTask tExcTask tTelnetd** **Non-Critical Task: tTest**
auditHistoryShow	Displays the contents of the audit.his file.
auditRebootSet 0/1	Globally disables the card reboot from this audit task. By default, this is set to 1. If it is set to 0, no card reboot occurs when a suspended task is found for critical or non-critical tasks. The debug information is dumped; however, recovery requires a manual reset of the card.

Table 27
Maintenance Audit commands (Part 2 of 2)

Command	Description
auditRebootTimeSet "timeString"	Sets the reset time for non-critical tasks to the value defined by the timeString parameter. The timeString is formatted as HH:MM and is in 24-hour clock format. By default, the time is set to 02:00 (2 AM).
auditTaskSet tTaskName, 0/1	Forces a task to be considered critical or non-critical. This command overrides the audit's default setting for the task. The tTaskName parameter specifies the task (the VxWorks taskname), as displayed by the "i" command. The value of 0 marks the task as non-critical, the value of 1 marks it as critical.

Hardware Watchdog Timer

A hardware watchdog timer is enabled on the ITG-P Line Card and Succession Media Card. This functionality adds further robustness to the existing exception handler and maintenance task audits.

The hardware watchdog timer handles scenarios such as the following:

- the CPU failing
- the code running and not triggering an exception
- resetting the card and bringing it back to normal operation

The timer runs on the ITG-P Line Card and Succession Media Card processors. The card's main processor is polled every 20 seconds. If three pollings are missed, then the card is reset. This gives the main processor 60 seconds to respond, covering most normal operating conditions.

A reset reason is saved when a card resets. The reset reason is displayed as a message during the startup sequence and appears in the SYSLOG file.

The following are examples of reset reasons:

- JAN 04 12:17:45 tXA: Info Last Reset Reason: Reboot command issued
  Output after card reset using the CLI command cardReboot.
- JAN 04 12:17:45 tXA: Info Last Reset Reason: Watchdog Timer Expired
  Output after card reset due to watchdog timer expiration.
- JAN 04 12:17:45 tXA: Info Last Reset Reason: Manual reset
  Output after card reset due to either the faceplate reset button press or a power cycle to the card.
- JAN 04 12:17:45 tXA: Info Last Reset Reason: Unknown
  Output after card reset due either the card F/W not supporting the reset reason or a corruption of the reset reason code.

The last reset reason can also be displayed at any time by entering the lastResetReason CLI command.

The Watchdog Timer and the Voice Gateway Media Card firmware

The application starts the Watchdog Timer as part of the application startup process. The timer is started only if the application's check of the firmware version indicates the card's firmware supports the Watchdog Timer function.

Required Voice Gateway Media Card firmware version

A firmware upgrade can be required on the Voice Gateway Media Cards to invoke the Watchdog Time functionality:

- ITG-P Line Card – Version 5.3 of the firmware file is the required minimum to enable the Watchdog Timer functionality on the ITG-P Line Card. To upgrade the firmware version of the ITG-P Line Cards to support the Watchdog functionality, see Procedure 90 on page 590.
- Succession Media Card–Version 6.0 of the firmware file is the required minimum to enable the Watchdog Timer functionality on the Succession Media Cards. To upgrade the firmware version of the Succession Media Card to support the Watchdog functionality, see Procedure 91 on page 592.

Codecs

Codec refers to the voice coding and compression algorithm used by the DSPs on the Voice Gateway Media Card. Different codecs provide different levels of voice quality and compression properties. The specific codecs and the order in which they are used, are configured in the TPS and Meridian 1 and Succession CSE 1000.

Table 28 on page 118 shows which codecs are supported on the Meridian 1 and Succession CSE 1000 Rel 1.1 systems, and on the Succession CSE 1000 Rel 2.0 systems:

Table 28
Supported codecs

Codec	Supported on Meridian 1 and Succession CSE 1000 Rel 1.1	Supported on Succession CSE 1000 Rel 2.0
G.711	Yes	Yes
G.729A	Yes	Yes
G.729AB	Yes	Yes
G.723.1	No	Yes
T.38	No	Yes
G.711 Clear Channel	No	Yes

Note 1: The G.723.1 codec is supported only on Succession CSE 1000 Release 2.0 system. The supported G.723.1 codec has bit rates of 5.3 Kbps and 6.3 Kbps. The user can configure the G.723.1 codec with a 5.3 Kbps bit rate; however, the system accepts both G.723.1 5.3Kbps and 6.4Kbps from the far end.

Note 2: The T.38 and G.711 Clear Channel codecs are supported for fax calls and are supported only on the Succession CSE 1000 Release 2.0 system. T.38 is the preferred codec type for fax calls over virtual trunks. However, the G.711 Clear Channel codec is used if the far end does not support the T.38 codec.

For detailed information about codecs, refer to “Codecs” on page 140.

Capacity Engineering Guidelines

Contents

This section contains information on the following topics:

Reference list

The following are references for this section:

- *Capacity Engineering* (553-3001-149)
- *Features and Services* (553-3001-306)
- *Planning and Engineering Guidelines* (553-3023-102)

Overview

This chapter provides capacity engineering guidelines to help plan and engineer the Meridian 1 and Succession Communication Server for Enterprise 1000 to support the ITG-P Line Card and the Succession Media Card, as well as the i2002 and i2004 Internet Telephones, and the i2050 Software Phone.

Refer to "IP Network Engineering Guidelines" on page 133 for IP Network Engineering information.

Refer to "Configuration of the DHCP Server" on page 211 for engineering guidelines to set and configure the Dynamic Host Configuration Protocol (DHCP) server to support the Voice Gateway Media Card and Internet Telephones.

Capacity engineering

This section explains how to calculate Meridian 1 and Succession CSE 1000 system capacity when engineering the ITG-P Line Card and Succession Media Card for an Internet Telephone.

IP Line capacity

Table 29 lists the system IP Line capacity for cards, telephones, and gateway ports.

Table 29
System IP Line capacity (Part 1 of 3)

Parameter	Capacity
ITG-P Line Cards in each system	Each card requires **two** slots (subject to EMC restriction, see "Electro-magnetic compatibility (EMC)" on page 672)
— Option 11C or 11C-Mini	— Option 11C - 2 cards in each cabinet (Class B rating) — Option 11C-Mini - 2 cards in each cabinet combination (Main + Expansions) (Class B rating)
— Option 51C, 61C, 81C, and 81C CPPII	— 4 cards in each IPE cabinet (Class B rating)
— Succession CSE 1000 Release 1.1	— 2 cards in each Media Gateway and 2 cards in each Media Gateway Expansion (Class A rating)
— Succession CSE 1000 Release 2.0	— 2 cards in each Media Gateway and 2 cards in each Media Gateway Expansion (Class A rating)

Table 29
System IP Line capacity (Part 2 of 3)

Parameter	Capacity
Succession Media Cards in each system	Each card requires **one** slot (subject to EMC restriction, see "Electro-magnetic compatibility (EMC)" on page 672)
— Option 11C or 11C-Mini	— No limit (Class B rating)
— Option 51C, 61C, 81C, and 81C CPPII	— Maximum of 10 cards for each IPE cabinet (Class B rating) with nor more than 3 cards per superloop
— Succession CSE 1000 Release 1.1	— No limit (Class A rating)
— Succession CSE 1000 Release 2.0	— No limit (Class A rating) of cards for each cabinet but it is recommended that no more that 4 Succession Media Cards in each Media Gateway since other slots are needs for PSTN trunking, etc.

Table 29
System IP Line capacity (Part 3 of 3)

Parameter	Capacity
Internet Telephone on each Voice Gateway Media Card	
— ITG-P Line Card	Maximum of 96 telephones supported on each ITG-P Line Card.
— Succession Media Card	Maximum of 128 telephones supported on each Succession Media Card.
Gateway ports on each Voice Gateway Media Card	
— ITG-P Line Card	— Maximum of 24 IP to circuit-switched gateway ports on each card.
— Succession Media Card	— Maximum of 32 IP to circuit-switched gateway ports on each card.
Internet Telephones in the System	
— Option 11C or 11C-Mini	— 640
— CP3	— 1000
— CP4	— 1000
— CPP	— 2000
— Succession CSE 1000 Rel 1.0 and Succession CSE 1000 Rel 1.1	— 640
— Succession CSE 1000 Rel 2.0	— 1000

Capacity engineering considerations

Number of Internet Telephones in the system

- **Option 11C or 11C-Mini** - There is a maximum of 640 Internet Telephones for an Option 11C or 11C-Mini. A maximum of five virtual superloops, 96-112 with cards 61-80 (640 telephones).
- **Option 51C, 61C, 81C, and 81C CPPII** - The number of Internet Telephones is determined by the engineering of real time usage, traffic capacity, network loop usage, and IPE slot usage, up to the maximum stated in Table 29 on page 121 for the specific CPU type.
- **Succession CSE 1000 Release 1.1** - There is a maximum of 640 Internet Telephones.
  - For normal traffic engineering, provision up to 1024 virtual TNs for each virtual superloop.
  - For a non-blocking virtual superloop configuration, do not exceed 120 virtual TNs for each virtual superloop.
  - A maximum of five virtual superloops, 96-112 with cards 61-80 (640 Internet Telephones).

  Note 1: In Option 51C/61C/81/81Cs, virtual superloops contend for the same range of loops with phantom, DECT, standard, and remote superloops, digital trunk loops and all service loops.

  Note 2: Virtual superloops, phantom superloops, and DECT superloops contend for the same five superloops in Option 11C/11C-Mini.
- **Succession CSE 1000 Release 2.0** - There is a maximum of 1000 Internet Telephones. Up to 1024 VTNs can be configured on a single virtual superloop for Succession CSE 1000 Rel 2.0. Table 8 on page 47 describes the virtual superloop and virtual card mapping on a Succession CSE 1000 Rel 2.0 system.

For more information on configuring virtual superloops, see “Configure virtual superloops for Internet Telephones (LD 97)” on page 259.

Maximum number of Voice Gateway Media Cards in the system

Table 29 on page 121 describes the number of ITG-P Line Cards and Succession Media Cards that can be installed in a system.

Other Considerations

On a traditional telephone, the tones are generated by Meridian 1 and Succession CSE 1000. The Internet Telephone can generate tones that originate on the original switch, so the tones are not affected by distortion caused by compression codecs such as G.729A.

Traffic capacity of Voice Gateway Media Cards when supporting Internet Telephones

Each ITG-P card has 24 ports that are used for establishing a voice connection between Internet Telephones and non-Internet Telephones (such as digital telephones or public network). To configure a system as non-blocking (as is typically the case for ACD configurations), ensure only 24 Internet Telephones are registered on each card.

Each Succession Media card has 32 ports that can be used for establishing a voice connection between Internet Telephones and non-Internet Telephones. To configure a system as non-blocking (as is typically the case for ACD configurations), ensure that only 32 Internet Telephones are registered on each card.

A registered telephone is not synonymous with a configured telephone. When a telephone is registered, it is as if the telephone is plugged in. When the telephone de-registers, it is as though the telephone is unplugged. Registration consists of two steps:

1 Verifying the user's TN is valid and has not yet been registered.

2 Associating the TN on the Meridian 1 and Succession CSE 1000 side.

If an Internet Telephone is unplugged, it is automatically un-registered after a pre-determined time-out. This limitation on simultaneous calls depends on the number and type of calls (not on the number of ports).

A call between two Internet Telephones on the same Meridian 1 or Succession CSE 1000 IP Telephony node does not use the Voice Gateway Media Card as a voice path across the data network.

Voice Gateway Media Cards in a Meridian 1 and Succession CSE 1000 are pooled by customer number, are assigned dynamically, and are allocated preferentially by matching bandwidth management zones. For more details, see “VoIP bandwidth management zones” on page 164. An Internet Telephone can be assigned any port of any Voice Gateway Media Card within the Meridian 1 and Succession CSE 1000 system.

> ***Note:*** The average number of Busy Hour Call Attempts must not exceed an average of 1200 BHCA each hour.

Refer to the following three examples for further clarification:

Example 1:

150 Internet Telephones with "typical" business usage of 600 call seconds per hour (CCS) for each telephone on average (for example, 5 calls of 120 seconds duration per hour)

- 150 x 6 CCS = 900 CCS
- 2 ITG-P Line Cards or 2 Succession Media Cards are required. Refer to Table 30 on page 129:
  - — 2 ITG-P Line Cards support up to 1232 CCS
  - — 2 Succession Media Card support up to 1738 CCS

Example 2:

500 telephones with "heavy" business usage of 12 CCS for each telephone on average (for example, 6-7 calls of 180 seconds duration every hour)

- 500 x12 CCS = 6000 CCS
- 8 ITG-P Line Cards or 6 Succession Media Cards are required. Refer to Table 30 on page 129:
  - — 8 ITG-P Line Cards support up to 6013 CCS
  - — 6 Succession Media Cards support up to 6013 CCS

Example 3:

48 Call Center Agents with an allocation of 36 CCS for each telephone

- 2 ITG-P Line Cards or 2 Succession Media Cards are required
  - — 48 ports required / 24 ports for each ITG-P Line Card = 2 ITG-P Line Cards
  - — 48 ports required / 32 ports for each Succession Media Card = 2 Succession Media Cards (1.5 must be rounded up to 2)

Note: For Call Center Agents, it is recommended that one port be provisioned for each agent.

ISM parameters

Customers must purchase one Internet Telephone ISM parameter for each Internet Telephone installed on Meridian 1 and Succession CSE 1000 systems. A new ISM parameter uses the existing Meridian 1 and Succession CSE 1000 keycode to enable the Internet Telephone in the system software. The default is zero.

For a Meridian 1 system, the required ISM parameter depends on the system configuration:

- NTZC82AA Internet Telephone Software Parameter (Option 51C, 61C, 81C, and 81C CP PII System)
- NTZC84AA Internet Telephone Software Parameter (Option 11C/11C-Mini System)

For a Succession CSE 1000 system, the required ISM parameter depends on the system configuration:

- NTM450AA Basic
- NTM451AA Advanced
- NTM452AA Premium

If you expand the ISM limits for the Internet Telephones, you must order and install a new Meridian 1 or Succession CSE 1000 keycode. Refer to the Incremental Software Management feature module in the *Features and Services* (553-3001-306) NTP.

> ***Note:*** Individual ISMs are not supported on Functional Pricing. With Functional Pricing, ISMs are provisioned in blocks of eight.

Internet Telephone Engineering

Traffic and Service Circuits

Virtual loops use software resources for tracking speech path traffic usage and Call Detail Recording. There are 120 of these resources for each virtual loop. The engineering of Internet Telephones is similar to that for existing digital telephones (based on 3500 CCS for each virtual loop).

The Voice Gateway Media Card's gateway channels are engineered the same as trunks between the circuit-switching fabric and the IP network. The TDS/Conference circuits are engineered for Internet Telephones as well as for existing digital telephones (one TDS/CONF card for each half group of Internet Telephones).

Gateway Channels Traffic Engineering

Configure no more than five Voice Gateway Media Cards on each superloop to eliminate the possibility of blocking because of insufficient talkslots (for example, 5 Voice Gateway Media Cards x 24 ports = 120 talkslots). Use Table 30 to determine the number of Voice Gateway Media Cards required to maintain the recommended capacity.

Table 30
Voice Gateway Media Card recommendations based on CCS capacity (Part 1 of 2)

The Internet Telephone blocking probability is 0.005.		
Number of Cards	**ITG-P Line Card CCS Capacity**	**Succession Media Card CCS Capacity**
1	511	744
2	1232	1738
3	1996	2780
4	2780	3845
5	3577	4924
6	4383	6013
7	5196	7110
8	6013	8212
9	6835	9318
10	7660	10429
11	8488	11542
12	9318	12658
13	10144	13777
14	10983	14897
15	11818	16020

Table 30
Voice Gateway Media Card recommendations based on CCS capacity (Part 2 of 2)

The Internet Telephone blocking probability is 0.005.		
Number of Cards	**ITG-P Line Card CCS Capacity**	**Succession Media Card CCS Capacity**
16	12657	17144
17	13496	18269
18	14335	19396
19	15177	20524
20	16020	21653

Note 1: CCS is the number of hundred call seconds per hour.

Note 2: If the number of ITG-P Line Cards exceeds 20, add 801 CCS to the total capacity for each additional card.

Note 3: If the number of Succession Media Cards exceeds 20, add 1082 CCS to the total capacity for each additional card.

Real time factors

The real time factors for Internet Telephones are provided in Table 31.

Table 31
Real time factors for Internet Telephones

Call scenario	Real time Factors for ITG-P Line Card	Real time Factors for Succession Media Card
1 - way inbound	0.78	1.75
1 - way outbound	1.59	1.75
2 - way	2.95	2.00

The total real time capacity of the Meridian 1 and Succession CSE 1000 depends on factors such as:

- calling patterns
- feature operations
- telephone and trunk signaling
- system CPU capacity

These factors are used to provision the maximum number of Internet Telephones supported on specific Meridian 1 and Succession CSE 1000 systems. These factors also describe the impact of using Internet Telephones relative to real time usage for a basic call between two 2500 telephones.

For Meridian 1 and Succession CSE 1000 Rel 1.0 and 1.1 systems, refer to *Capacity Engineering* (553-3001-149) for further information. For Succession CSE 1000 Rel 2.0 systems, refer to *Planning and Engineering Guidelines* (553-3023-102) for further information.

Product compatibility with other IP products

Nortel Networks supports the following Voice Over IP (VoIP) products in addition to the IP Line. These products are:

- Meridian 1 Internet Telephony Gateway Trunk 2.0 card/ISDN Signaling Link
- Meridian 1 Internet Telephony Gateway Trunk 2.1 card/ISDN Signaling Link
- 802.11 Wireless IP Gateway

Each IP product uses TLANs and ELANs that can co-exist with each other. All cards within a node must be on the same TLAN subnet. They can share the same TLANs, and must share the same ELAN. You need to engineer the traffic on the TLAN to consider all IP applications.

For EMC compliance, add up all the IP products to stay within EMC limits.

IP Network Engineering Guidelines

Contents

This section contains information on the following topics:

Reference list

The following are the references for this section:

- *Software Input/Output: Administration* (553-3001-311)
- *Data Networking Guidelines* (553-3023-103)

Overview

This chapter provides guidelines and recommendations to help plan, engineer, and test the Voice Gateway Media Card and Internet Telephone network on the Meridian 1 system.

For Succession Communication Server for Enterprise (CSE) 1000 Release 2.0 systems, also refer to *Data Networking Guidelines* (553-3023-103).

The following procedures are contained within this chapter:

- Procedure 1, "Performing the Network assessment procedure" on page 138
- Procedure 2, "Calculating TLAN traffic" on page 156
- Procedure 3, "Calculating WAN traffic" on page 161
- Procedure 4, "Assessing link utilization" on page 167

See "Configuration of the DHCP Server" on page 211, for engineering guidelines to set up and configure the Dynamic Host Configuration Protocol (DHCP) server to support the Voice Gateway Media Card and Internet Telephones.

IP address requirements

This section describes the IP address requirements for each node, for each card, and for each Internet Telephone.

A node is a group of ITG-P Line Cards and Succession Media Cards within a given Meridian 1 or Succession CSE 1000 system. Each card within a node has two IP addresses: a node for the Telephony LAN (TLAN) and a node for the Meridian 1 or Succession CSE 1000 Embedded LAN (ELAN). Each node has one Node IP address on the TLAN, that is dynamically assigned to the connection server on the node Master. The Internet Telephone uses the Node IP address during the registration process.

All ELAN addresses for all nodes must be on one subnet. All ELAN addresses must be on the same subnet as the Meridian 1 or Succession CSE 1000 Core ELAN. All TLAN addresses must be in the same subnet for a given node.

General Requirements for a Node's IP Addressing

The following is a list of IP addresses that must be assigned to configure a node:

- IP address for every TLAN interface of every Voice Gateway Media Card
- IP address for every ELAN interface of every Voice Gateway Media Card
- Voice LAN (TLAN) Node IP address (This address is shared among all the cards.) This alias IP address appears dynamically on the TLAN port of one card in the node, the Leader or node Master.
- On the Succession CSE 1000 Rel 2.0 system, an IP address for the Signaling Server ELAN and Signaling Server TLAN

In addition to the IP addresses that must be assigned, additional network information must be entered:

- Management LAN (ELAN) gateway IP address
- Management LAN (ELAN) subnet mask
- Voice LAN (TLAN) subnet mask
- VLAN gateway IP address

CAUTION
You must use separate subnets with the Voice Gateway Media Card for ELAN and TLAN.

The default setting of separate ELAN and TLAN subnets offers the following benefits:

- Separate subnets are easier to configure for traffic management and Quality of Service (QoS).
- Separate subnets protect the Meridian 1 and Succession CSE 1000 ELAN from general LAN traffic, including broadcast and multicast storms
- Separate subnets are more secure against unauthorized access

Voice Gateway Media Card IP address requirements

The IP address information for each card is set in the **Configuration** tab of the **ITG Node Properties** window of the IP Telephony Gateway - IP Phones application. The IP address requirements for each card depend on the node subnet option.

You must provide an IP address for an ELAN and TLAN port. On the ELAN, all cards must be on the same subnet, which is the same subnet that the Meridian 1 and Succession CSE 1000 is connected to. On the TLAN, all cards in a node must be on the same subnet.

The ELAN address corresponds to the Management MAC address which is assigned during manufacturing and cannot be changed. Locate the faceplate sticker on the Voice Gateway Media Card. The ELAN/Management MAC address is the MOTHERBOARD Ethernet address.

Separate subnet Voice Gateway Media Card IP address requirements

You must use separate subnets for the IP Telephony node. Each Voice Gateway Media Card requires a:

- Management IP address
- Voice IP address
- Management MAC
- Voice LAN gateway IP address

IP network assessment procedure

An efficient IP Line network design begins with an understanding of traffic and the underlying network that carries the traffic. To determine the network requirements of the specific system, the technician must perform the steps in Procedure 1.

Procedure 1
Performing the Network assessment procedure

1 Estimate the amount of traffic processed by the Meridian 1 or Succession CSE 1000 system through the IP Line network. See "Calculate IP Line traffic requirements" on page 155.

2 Assess if the existing corporate intranet can adequately support voice services. See "Calculate IP Line traffic requirements" on page 155 and "Assess WAN link resources" on page 161.

3 Organize the IP Line network into "zones" representing different topographical areas of the network that are separated according to bandwidth considerations. See "VoIP bandwidth management zones" on page 164.

4 Set a variety of service parameters to improve service and coordinate (with the IP administrator) the prioritization of voice packets with data traffic. See "Set service parameters" on page 171.

5 Provide the necessary IP network infrastructure:

a. 10BaseT or 100BaseTX Ethernet connection.

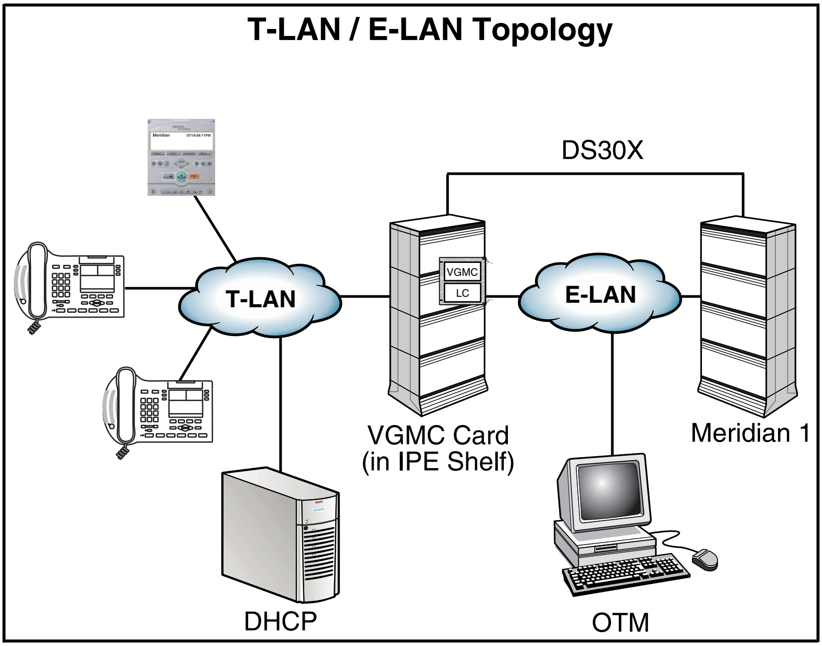
b. IP address. Each Voice Gateway Media Card requires 10BaseT ELAN or 10/100BaseT TLAN unicast IP address.

c. One additional IP address for each node. The node IP address is the TLAN for a subnet.

End of Procedure

After completing the network assessments, the technician can design and implement the IP Line network. This can involve modifications to both the IP Line elements and to the existing network. Post-installation network measurements (see page 191) must be made on a regular basis to make sure QoS standards are maintained. Figure 6 shows an example of the TLAN and ELAN topology.

Figure 6
TLAN and ELAN Topology



Codecs

The Internet Telephones and Voice Gateway Media Cards support different codecs and codec parameters with different compression rates and audio quality. The Meridian 1 and Succession CSE 1000 selects the appropriate codecs based on user-configurable parameters. For instance, an Internet Telephone-to-Internet Telephone within a LAN can be set up using G.711 at 64 Kbps. For an Internet Telephone-to-Internet Telephone call over a WAN, the call can be set up using G.729A or G.729AB at 8 Kbps. These data rates and the Voice Gateway Channel Server on the Voice Gateway Media Card are for the voice stream only. Packet overhead is not included.

The Terminal Proxy Server (TPS) and the Voice Gateway Channel Server on the Voice Gateway Media Card have a predefined table of codec option sets that can be supported. The first entry in the table has the highest quality audio (BQ = Best Quality) and requires the largest bandwidth. The last entry requires the least bandwidth (BB = Best Bandwidth) with lower voice quality.

When the Call Server sets up a Call Server connection between an Internet Telephone-to-Internet Telephone or Internet Telephone-to-Voice Gateway Channel Server, the predefined table determines which codec it selects for that connection. This information is provided to the Meridian 1 and Succession CSE 1000 as part of the Internet Telephone registration sequence. For more information about the registration sequence, refer to "Configuration of the DHCP Server" on page 211. The Meridian 1 and Succession CSE 1000 use this information to set up a speech path to select a codec that both endpoints support. As part of zone management, it further selects the codec based on whether it is trying to optimize quality (BQ) or bandwidth (BB).

CAUTION
When voice compression codecs are used, voice quality is impaired if end-to-end calls include multiple compressions.

Codec refers to the voice coding and compression algorithm used by the DSPs on the Voice Gateway Media Card. Different codecs provide different levels of voice quality and compression properties. The specific codecs and the order in which they are used are configured in the TPS, and Meridian 1 and Succession CSE 1000.

Table 32 shows which codecs are supported on the Meridian 1 and Succession CSE Rel 1.1 systems, and on the Succession CSE 1000 Rel 2.0 systems:

Table 32
Supported codecs

Codec	Supported on Meridian 1 and Succession CSE 1000 Rel 1.1	Supported on Succession CSE 1000 Rel 2.0
G.711	Yes	Yes
G.729A	Yes	Yes
G.729AB	Yes	Yes
G.723.1	No	Yes
T.38	No	Yes
G.711 Clear Channel	No	Yes

Note 1: The G.723.1 codec is supported only on Succession CSE 1000 Release 2.0 system. The supported G.723.1 codec has bit rates of 5.3 Kbps and 6.3 Kbps. The user can configure the G.723.1 codec with a 5.3 Kbps bit rate; however, the system accepts both G.723.1 5.3Kbps and 6.4Kbps from the far end.

Note 2: The T.38 and G.711 Clear Channel codecs are supported for fax calls and are only supported on the Succession CSE 1000 Release 2.0 system. T.38 is the preferred codec type for fax calls over virtual trunks. However, the G.711 Clear Channel codec is used if the far end does not support the T.38 codec.

Table 33 lists the payload sizes for the different codecs:

Table 33
Codec payload sizes

Codec	Payload
G.711	10ms, 20ms, 30ms
G.729A	10ms, 20ms, 30ms, 40ms, 50ms
G.729AB	10ms, 20ms, 30ms, 40ms, 50ms
G.723.1	30ms
T.38	supported for fax calls
G.711 Clear Channel	supported for fax calls

Note: If there are multiple nodes on a system and the same codec is selected on more than one node, ensure that each node has the same voice payload size configured for the codec.

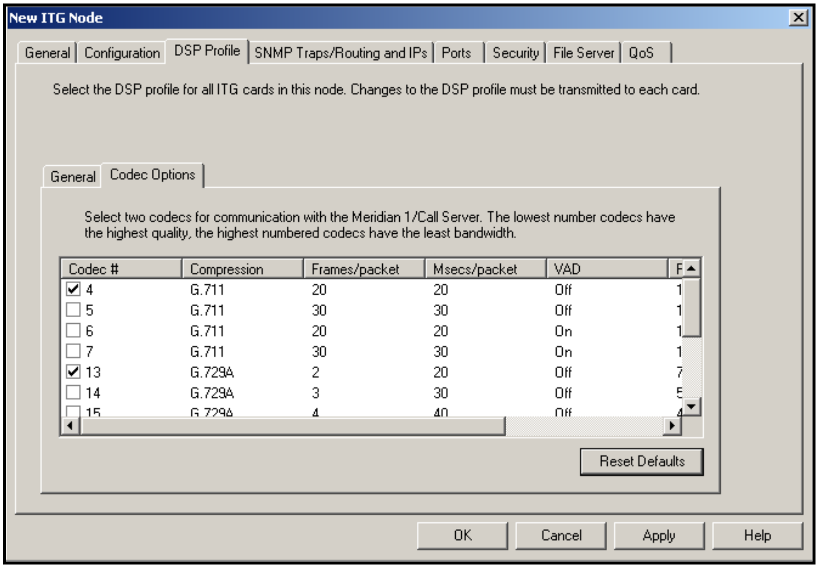
Codec configuration

Configure codec in the DSP Profile sections of OTM and Element Management.

Meridian 1 and Succession CSE 1000 Rel 1.1

Figure 7 on page 143 shows the list of codecs available on the DSP Profile tab within OTM's ITG Line 3.0 application. The Codec Options sub-tab presents a table of different sets of codec options identified by a codec setting index number. There is a list of up to 32 codec settings for G.711, G.729A, and G.729AB. The lesser codec setting index corresponds to BQ (Best Quality) in LD 117 zone configuration. The greater codec setting index corresponds to BB (Best Bandwidth). For more information, see"Codec selection" on page 191.

Figure 7
Codec list on OTM 2.0

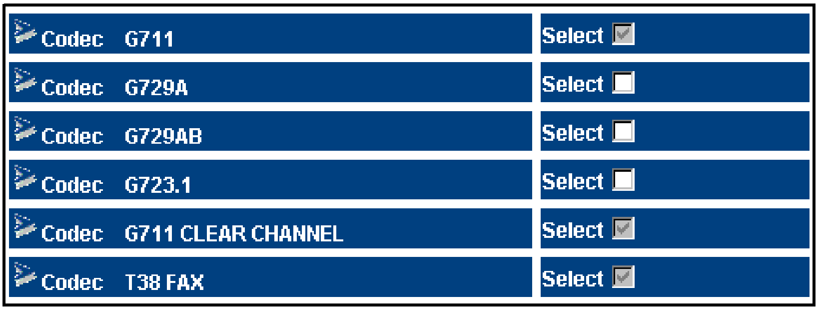


For codec configuration in the Meridian 1 and Succession CSE 1000 Rel 1.1 systems, see “Configuring DSP profile data” on page 284.

Succession CSE 1000 Rel 2.0

Figure 8 on page 144 shows the list of codec types that are displayed in the Element Management.

Figure 8
Codec list in Element Management



The G.711, G.711 Clear Channel, and T.38 Fax codecs are automatically selected and cannot be unselected. Even though these codecs cannot be unselected, the payload size, and the jitter buffer for G.711 can be changed. For G.711 Clear Channel, only the jitter buffer can be changed.

The user can select all three, any two, any one, or none of the G.729A, G.729AB, and G.723.1 codecs. If the G.729A or G.729AB codec is selected, the user can change the payload size and the jitter buffer. If the G.723.1 codec is selected, the user can change only the jitter buffer, because the only supported payload size is 30 msec.

For codec configuration in the Succession CSE 1000 Rel 2.0 system, see “Configuring DSP Profile data” on page 346.

Codec Registration on Succession CSE 1000 Rel 2.0

After the configuration of codecs is complete, the Internet Telephones and DSPs have to register the configured codecs with the Call Server.

Codec registration for Internet Telephones

The Internet Telephones register both the G.711 a-law and mu-law codecs, and any codec(s) configured by the user. The codecs that can be configured by the user are G.729A, G.729AB, and G.723.1.

> ***Note:*** Internet Telephones do not register the fax codecs (T.38 and G.711 Clear Channel).

The minimum number of codecs registered for an Internet Telephone is two: G.711 a-law and G.711 mu-law (G.711 is always configured).

The maximum number of codecs registered for an Internet Telephone is five: G.711 a-law, G.711 mu-law, G729A, G729AB, and G.723.1.

Example 1

A user configures a G.711 mu-law codec (with a 30 msec payload) and a G.723.1 codec (with a 30 msec payload).

The following three codecs are actually registered:

1. G.711 mu-law (30 msec)
2. G.711 a-law (30 msec)
3. G.723.1 (30 msec)

Example 2

A user configures four codecs:

1. G.711 a-law codec with a 10 msec payload
2. G.729A codec with 50 msec payload
3. G.729AB codec with 30 msec payload
4. G.723.1 codec with a 30 msec payload

The following five codecs are actually registered:

1. G.711 a-law (10 msec)
2. G.711 mu-law (10 msec)
3. G.729A (50 msec)
4. G.729AB (30 msec)
5. G.723.1 (30 msec)

Codec registration for DSPs

DSPs register the following codecs:

- both G.711 a-law and G.711 mu-law codecs
- both fax codecs (T.38 and G.711 Clear Channel)
- one best bandwidth (BB) codec if at least one of G.729A, G.729AB, or G.723.1 codecs was configured by the user. The best bandwidth (BB) codec is based on the codec type. The order of preference for choosing the best bandwidth codec is G.729AB, G.729A, and then G.723.1.

The minimum number of codecs registered for DSPs is four: G.711 a-law, G.711 mu-law, T.38 and G.711 Clear Channel.

The maximum number of codecs registered for DSPs is five: G.711 a-law, G.711 mu-law, T.38 and G.711 Clear Channel and one of G.729AB, G.729A, or G.723.1.

Example 1

A user configures four codecs:

1. G.711 a-law codec with a 10 msec payload
2. G.729A codec with 50 msec payload
3. G.729AB codec with 30 msec payload
4. G.723.1 codec with a 30 msec payload

The following five codecs are actually registered:

1 G.711 a-law (10 msec)

2 G.711 mu-law (10 msec)

3 G.729AB (30 msec)

4 T.38

5 G.711 Clear Channel

The G.729AB codec is selected, as it is the first in the order of preference of the “best bandwidth” codecs. The G.729A and G.723.1 codecs do not get registered.

Example 2

A user configures three codecs:

1 G.711 mu-law codec with a 20 msec payload

2 G.729A codec with 30 msec payload

3 G.723.1 codec with a 30 msec payload

The following five codecs are actually registered:

1 G.711 mu-law (20 msec)

2 G.711 a-law (20 msec)

3 G.729A (30 msec)

4 T.38

5 G.711 Clear Channel

The G.729A codec is selected, as it precedes the G.723.1 codec in the order of preference of the “best bandwidth” codecs.

Codec negotiation for Succession CSE 1000 Rel 2.0

For every virtual trunk call, a common codec must be selected for the call. This is known as codec negotiation. Codec negotiation for virtual trunk calls is performed through the H.323 FastStart and Terminal Capability Set (TCS) messages.

For a call setup with the FastStart procedure, the originating node sends its codec list in the FastStart element in the SETUP message to the terminating node. For a call setup using the SlowStart procedure or for a call modification (media redirection), each node sends its codec list in the TCS message to the other node.

Before sending a codec list in FastStart and TCS messages, the codec list must be sorted according to the Best Bandwidth or Best Quality policy. This is determined by the following:

- the zone configuration of the Internet Telephone / DSP involved in the call
- the zone configuration of the virtual trunk used for the call

Codec list sorting

There are two methods for sorting the codec list:

1. Best Quality (BQ) sorting - The codec list is sorted so that the first codec in the list is the best quality codec, the second codec is the second best quality codec in the list, and so on.
2. Best Bandwidth (BB) sorting - The codec list is sorted so that the first codec in the list is the best bandwidth codec, the second codec is the second best bandwidth codec in the list, and so on.

Table 34 on page 149 shows the codec list sorting order for the BQ and BB codecs. To know if a codec is best quality (as compared to another codec), refer to the lists in columns 1 and 2. To know if a codec is best bandwidth (as compared to another codec), refer to the lists in columns 3 and 4. The best quality or bandwidth codec is listed at the top of the column.

Table 34
BQ and BB codec sorting lists

Best Quality (BQ) Sorting		Best Bandwidth (BB) Sorting	
For mu-law systems	**For a-law systems**	**For mu-law systems**	**For a-law systems**
G.71_mu_law_10msec	G.711_a_law_10msec	G.729AB_50msec	G.729AB_50msec
G.711_mu_law_20msec	G.711_a_law_20msec	G.729AB_40msec	G.729AB_40msec
G.711_mu_law_30msec	G.711_a_law_30msec	G.729AB_30msec	G.729AB_30msec
G.711_a_law_10msec	G.711_mu_law_10msec	G.729AB_20msec	G.729AB_20msec
G.711_a_law_20msec	G.711_mu_law_20msec	G.729AB_10msec	G.729AB_10msec
G.711_a_law_30msec	G.711_mu_law_30msec	G.729A_50msec	G.729A_50msec
G.729A_10msec	G.729A_10msec	G.729A_40msec	G.729A_40msec
G.729A_20msec	G.729A_20msec	G.729A_30msec	G.729A_30msec
G.729A_30msec	G.729A_30msec	G.729A_20msec	G.729A_20msec
G.729A_40msec	G.729A_40msec	G.729A_10msec	G.729A_10msec
G.729A_50msec	G.729A_50msec	G.723.1_5.3kbps_30ms	G.723.1_5.3kbps_30ms
G.729AB_10msec	G.729AB_10msec	G.723.1_6.4kbps_30ms	G.723.1_6.4kbps_30ms
G.729AB_20msec	G.729AB_20msec	G.711_mu_law_30msec	G.711_a_law_30msec
G.729AB_30msec	G.729AB_30msec	G.711_mu_law_20msec	G.711_a_law_20msec
G.729AB_40msec	G.729AB_40msec	G.711_mu_law_10msec	G.711_a_law_10msec
G.729AB_50msec	G.729AB_50msec	G.711_a_law_30msec	G.711_mu_law_30msec
G.723.1_5.3kbps_30ms	G.723.1_5.3kbps_30ms	G.711_a_law_20msec	G.711_mu_law_20msec
G.723.1_6.4kbps_30ms	G.723.1_6.4kbps_30ms	G.711_a_law_10msec	G.711_mu_law_10msec
T.38	T.38	T.38	T.38
G.711CC	G.711CC	G.711CC	G.711CC

Codec selection for Succession CSE 1000 Rel 2.0

For every virtual trunk call, a codec must be selected before the media path is opened.

When a call setup with the FastStart procedure is used, the terminating node selects a common codec and sends the selected codec to the originating node. For a call modification (media redirection) or for a call setup using the SlowStart procedure, the codec selection occurs on both nodes. Each node has two codec lists: its own list and the far-end's list. To select the same codec on both nodes, it is essential to use the same codec selection algorithm on both nodes.

For the codec selection, both the near- and far-end codec lists are retrieved:

- The far-end list is not modified because it is already sorted when it is received (in FastStart or TCS message).
- The near-end list is sorted and then expanded to include lower payloads, the same way it is done before sending the codec list in FastStart message.

The following conditions are met before codec selection occurs:

- There are two codec lists:
  - The near-end list is the codec list of the local unit.
  - The far-end list is the codec list received from the far end.
- Each codec list can contain more than one payload size for a given codec type. The codec list depends on the codec configuration.
- Each codec list is sorted by order of preference. The first codec in the near end list is the near end's most preferred codec and the first codec in far end list is the far end's most preferred codec, and so on.

Once the above conditions are met, a codec selection algorithm is used to select the codec to be used for a call. There are two different codec selection algorithms:

1 H.323's Master/Slave algorithm

2 Best Bandwidth Codec Selection algorithm

H.323's Master/Slave algorithm

The codec selection algorithm proposed by the H.323 standard involves a Master/Slave negotiation, initiated each time two nodes exchange their capabilities (TCS message). The Master/Slave information decides that one node is Master and the other node is Slave. The outcome of the Master/Slave negotiation is not known in advance, it is a random result: one node could be Master then Slave (or vice versa) during the same call.

- The Master node uses its own codec list as the preferred one. From the far-end list, it finds the common codec.

  The Master gets the first codec in its own list (Codec1). The Master then checks the far-end list to see if Codec1 is a common codec (that is, is Codec1 also listed in the far-end list). If Codec1 is common to both lists, Codec1 becomes the selected codec. Otherwise, the Master obtains the second codec from its own list and repeats the search in the far-end list, and so on.

- The node which is Slave uses the far end list as the preferred list. The Slave selects a codec from the far end list and then searches in its own list to find the common codec.

The issues caused by the Master/Slave algorithm are due to the random nature of the Master/Slave information. The codec that is selected and used during a virtual trunk call cannot be pre-determined. This issue can make bandwidth usage calculations and bandwidth management difficult.

Known issues include:

- After an on-hold and off-hold scenario (that triggers Master/Slave negotiation), the codec used for the restored call can be different than the codec used before the call was placed on hold. The Master/Slave information could have been changed when the call was on hold.
- Since the terminating end of a call is always the Master, a call from telephone1 (node1) to telephone2 (node2) can use a different codec than a call from telephone2 (node2) to telephone1 (node1).
- For tandem calls, the Master/Slave information is not relevant. That is, the Master/Slave information is designed to be used only between two nodes, not among three or more nodes. The Master/Slave algorithm makes the codec selection for tandem calls more complex and inefficient.

To solve the issues, another codec selection algorithm was needed. This new algorithm is called the Best Bandwidth Codec Selection algorithm and it is not based on the unpredictable Master/Slave information.

The new codec algorithm is used for virtual trunk calls between Nortel Networks equipment, since any change to the Master/Slave algorithm implies a change to the H.323 standard. However, the H.323's Master/Slave algorithm is used when there is a virtual trunk call between Nortel Networks equipment and third-party equipment.

Best Bandwidth Codec Selection algorithm

The Best Bandwidth Codec Selection algorithm was implemented to solve the issues caused by the H.323 Master/Slave algorithm. The Best Bandwidth algorithm selects one common codec based on two codec lists. With this algorithm, every time the selection is done using the same two lists, the selected codec is always the same.

The "Best Bandwidth" codec selection is based on the codec type only; it does not take into account the fact that some codecs, while generally using less bandwidth, consume more bandwidth than others at certain payload sizes.

- This algorithm obtains the first codec in the near-end list that is also in far end list (codec is the same type and has the same payload size). Call the selected codec C1.
- Get the first codec in far end list that is also in near-end list (same type, same payload size). This codec is C2.
- Between C1 and C2, the codec that is selected is considered as the best bandwidth codec type. To determine which codec type is the best bandwidth, the following rules are used:
  - a G.729AB codec is considered as Best Bandwidth compared to G.729A, G.723.1, G.711_muLaw, and G.711_aLaw codecs
  - a G.729A codec is considered as Best Bandwidth compared to G.723.1,G.711_muLaw, and G.711_aLaw codecs
  - a G.723.1 codec is considered as Best Bandwidth compared to a G.711_muLaw and G.711_aLaw codec
  - a G.711_muLaw codec is considered as Best Bandwidth compared to a G.711_aLaw codec

Table 35 shows the codec that would be selected between any two codecs. For example, if the two codecs are the G.729A and G.723.1, the selected codec is the G.729A.

Table 35
Best Bandwidth codec selection between any two codecs types

Codec type	G.711_aLaw	G.711_muLaw	G.729A	G.729AB	G.723.1
G.711_aLaw	G.711_aLaw	G.711_muLaw	G.729A	G.729AB	G.723.1
G.711_muLaw	G.711_muLaw	G.711_muLaw	G.729A	G.729AB	G.723.1
G.729A	G.729A	G.729A	G.729A	G.729AB	G.729A
G.729AB	G.729AB	G.729AB	G.729AB	G.729AB	G.729AB
G.723.1	G.723.1	G.723.1	G.729A	G.729AB	G.723.1

Calculate IP Line traffic requirements

The technician must forecast the hundreds of call seconds for each hour (CCS) traffic that the Meridian 1 and Succession CSE 1000 processes through the IP Line network. CCS traffic generated by an Internet Telephone is similar to that of a digital telephone. The following procedures calculate the bandwidth required to support given amounts of traffic.

The procedures require the following data:

- CCS/CCS rating of Internet Telephone
- number of Internet Telephones
- number of subnets/servers accessed by the Internet Telephones

Note: Base all traffic data on busy hour requirements.

The result of the calculation provides estimated values for the following:

- total TLAN bandwidth requirement
- WAN bandwidth requirement for each subnet or server/router

The technician must consider the impact of incremental IP Line traffic on routers and LAN resources in the intranet. LAN segments can become saturated, and routers can experience high CPU use. A customer must consider re-routing scenarios in a case where a link is down.

TLAN traffic calculations

To calculate the total TLAN requirement, add together all sources of traffic destined for the Internet Telephony network using the same LAN. The data rate for a TLAN is the total bit rate. The total subnet traffic is measured in Erlangs. An Erlang is a telecommunications traffic measurement unit and it is used to describe the total traffic volume of one hour. Network designers use these measurements to track network traffic patterns. To calculate the TLAN traffic, follow Procedure 2.

Procedure 2
Calculating TLAN traffic

1 Total subnet traffic is the sum of (measured in Erlangs):

- number of Internet Telephones × CCS/CCS rating)
- voice gateways on Voice Gateway Media Card
- WAN connection

Note: Each source of traffic has a different CCS rating. Calculate the subnet traffic for each source of traffic and add the amounts to get the total.

2 Use the number of Erlangs to calculate the equivalent number of lines by using the calculator at the following Web site:

http://www.erlang.com/calculator/erlb

Note: Assume a blocking factor of 1% (0.010).

3 Find the TLAN bandwidth use (Kbps) in Table 36 on page 158 based on the codec used for the traffic source.

4 Calculate the bandwidth of a subnet using the following calculation:

Bandwidth for each subnet equals the total number of lines multiplied by the TLAN bandwidth usage, that is:

Subnet bandwidth = Total number of lines x TLAN bandwidth usage

5 Repeat steps 1 to 4 for each subnet.

6 To calculate the total TLAN traffic, add the total bandwidth for each subnet calculation.

End of Procedure

Table 36 on page 158 lists the bandwidth consumed by the various payload sizes of each codec. The Call Server uses the values in the columns labeled "TLAN Bandwidth". It looks up these values and subtracts them from the available zone bandwidth to determine if a zone has sufficient bandwidth for the call.

The "TLAN Bandwidth" values contain the total IP and Ethernet packet overhead of 78 bytes, including the 8 byte preamble and minimum 12 byte inter-packet gap. These are often excluded from bandwidth calculations but must be included to give a true indication of the bandwidth used. The Call Server assumes a Half Duplex Ethernet connection (again, to cover the worse case), so the bandwidth values shown are twice what is normally listed for a Full Duplex link.

The columns labeled "Base WAN Bandwidth" provide the data for the payload plus IP overhead without the Ethernet interface overhead. This data provides the basis for any WAN bandwidth calculations. The overhead associated with the particular WAN facility, such as Frame Relay, is added to the base value to determine the total bandwidth used. The values shown are for a duplex link, so if the WAN facility is Half Duplex, the values should be doubled.

> ***Note:*** The Call Server is unaware of the particulars of the WAN facility and always uses the values shown in the "TLAN Bandwidth" columns.

Table 36
TLAN and WAN IP bandwidth usage for each bi-directional IP conversation

				TLAN Bandwidth		Base WAN Bandwidth	
Codec type	**Packet duration (ms)**	**Voice payload (bytes)**	**VAD**	**Peak bandwidth (Kbps)**	**Average bandwidth (Kbps)**	**Peak bandwidth (Kbps)**	**Average bandwidth (Kbps)**
G.711 (64 Kbps)	10	80	Off	252.80	252.80	96.00	96.00
	20	160	Off	190.40	190.40	80.00	80.00
	30	240	Off	169.60	169.60	74.67	74.67
G.729A (8 Kbps)	10	10	Off	140.80	140.80	40.00	40.00
	20	20	Off	78.40	78.40	24.00	24.00
	30	30	Off	57.60	57.60	18.67	18.67
	40	40	Off	47.20	47.20	16.00	16.00
	50	50	Off	40.96	40.96	14.40	14.40
G.729AB (8 Kbps)	10	10	On	140.80	84.48	40.00	24.00
	20	20	On	78.40	47.04	24.00	14.40
	30	30	On	57.60	34.56	18.67	11.20
	40	40	On	47.20	28.32	16.00	9.60
	50	50	On	40.96	24.58	14.40	8.64
G.723.1 (6.3 Kbps)	30	24	Off	54.40	54.40	17.07	17.07
G.723.1 (5.3 Kbps)	30	24	Off	54.40	54.40	17.07	17.07

Note 1: The bandwidth estimates in Table 36 on page 158 assume a Half Duplex LAN/WAN connection and show the total bandwidth (both directions) used. For a Full Duplex link, such as Full Duplex Ethernet, the table's bandwidth estimates should be divided by two to determine the bandwidth used in one direction. However, the Call Server assumes the worse case (Half Duplex) when calculating the bandwidth used for each call against a Zone's bandwidth capacity.

Note 2: The "TLAN Bandwidth" overhead is assumed to be for Ethernet connections and is comprised of 8 bytes of Ethernet Preamble, 14 bytes of Ethernet, 20 bytes of IP, 8 bytes of UDP, and 12 bytes of RTP Header, plus 4 bytes of Ethernet check sum and 12 bytes of inter-packet gap. The total packet payload overhead is 78 bytes.

Note 3: Different transport types have slightly different bandwidth requirements.

Note 4: The average bandwidth is reduced from the peak bandwidth by the use of silence suppression (VAD).

Note 5: The reduction due to VAD is assumed to be 40%.

Note 6: The "Base WAN Bandwidth" overhead includes only the IP packet overhead of 20 bytes of IP, 8 bytes of UDP, and 12 bytes of RTP Header. The total packet payload overhead is 40 bytes. The values shown are for a Full Duplex data rate. Double the values if the WAN facility is Half Duplex.

TLAN engineering example

The following is an example of calculating TLAN bandwidth assuming Half Duplex links.

1 Subnet A: 28 Internet Telephones x 6 CCS/36 = number of Erlangs

Using G.729AB 30 msec, TLAN bandwidth usage is 57.6 Kbps.

Subnet A bandwidth = 4.66 lines x 57.6Kbps = 268.4 Kbps

2 Subnet B: 72 Internet Telephones, average 5 CCS/Internet Telephone

Subnet B total Erlangs = 72 x 5/36 = 10

Subnet B bandwidth = 10 x 57.6 = 576 Kbps

3 Subnet C: 12 Internet Telephones, average 6 CCS/Internet Telephone

Subnet C total Erlangs = 12 x 6/36 = 2

Subnet C bandwidth = 2 x 57.6 = 115.2 Kbps

4 Calculate the TLAN Bandwidth by adding each subnet bandwidth:

TLAN Bandwidth = 268.4 + 576 + 115.2 = 959.6 Kbps

——————————— ***End of Example*** ———————————

Assess WAN link resources

If IP Line traffic is routed over an intranet, the technician must assess the status of the network. For a locally connected Internet Telephone, if calls are routed to the PSTN, the calls affect only the capacity of the TLAN.

When calls are routed through an intranet, WAN links are frequently the source of capacity problems in the network. Unlike LAN bandwidth, which is virtually free and easily implemented, WAN links take time to obtain financial approval, provision, and upgrade. It is important to assess the state of WAN links in the intranet prior to implementing the IP Line network.

WAN traffic calculations

For data rate requirements for the intranet route, calculation is based on duplex channels. The data rate for a WAN is the duplex data rate. For example, 128 Kbps on the LAN is equal to a 64 Kbps duplex channel on the WAN. Use the following procedure to calculate data rate requirements for the intranet route. The effects of Real-time Transport Protocol (RTP) header compression by the router are not considered in these calculations but must be included where applicable.

Procedure 3
Calculating WAN traffic

1 Total subnet traffic = Number of Internet Telephones × CCS/Internet Telephone.

2 Convert to Erlangs:

Total CCS / 36 (on the Half Duplex LAN)

3 Find WAN bandwidth usage (Kbps) from the “WAN Base Bandwidth” columns of Table 35 on page 154.

4 Bandwidth for each subnet = Total Erlangs × WAN bandwidth usage.

5 Multiply bandwidth of each subnet by 1.3 to adjust for traffic peaking.

6 Repeat the procedure for each subnet.

7 Adjust WAN bandwidth to account for WAN overhead depending on the WAN technology used:

- ATM (AAL1): multiply subnet bandwidth × 1.20 (9 bytes overhead/44 bytes payload)
- ATM (AAL5): multiply subnet bandwidth × 1.13 (6 bytes overhead/47 bytes payload)
- Frame Relay: multiply subnet bandwidth × 1.20 (6 bytes overhead/30 bytes payload – variable payload up to 4096 bytes)

Note: Each WAN link must be engineered to be no more than 80% of its total bandwidth if the bandwidth is 1536 Kbps or higher (T1 rate). If the rate is lower, up to 50% loading on the WAN is recommended.

End of Procedure

WAN engineering example

The following is an example of calculating the WAN bandwidth.

1 Subnet A: 36 Internet Telephones, average 6 CCS/Internet Telephone

- Total Erlangs = 36 x 6/36 = 6
- For G.729AB 50 msec, WAN bandwidth usage is 14.4 Kbps.
- Subnet A WAN bandwidth = 14.4 x 6 = 86.4Kbps
- Subnet A WAN bandwidth with 30% peaking
= 86.4 x 1.3
= 112.32 Kbps

2 Subnet B: 72 Internet Telephones, average 5 CCS/Internet Telephone

- Total Erlangs = 72 x 5/36 = 10
- Subnet B WAN bandwidth = 14.4 x 10 = 144 Kbps
- Subnet B WAN bandwidth with 30% peaking
= 144 x 1.3
= 187.2 Kbps

3 Subnet C: 12 Internet Telephones, average 6 CCS/Internet Telephone

- Total Erlangs = 12 x 6/36 = 2
- Subnet C WAN bandwidth = 14.43 x 2 = 28.8 Kbps
- Subnet C WAN bandwidth with 30% peaking
  = 28.8 x 1.3
  = 37.44 Kbps

4 If the WAN is known to be an ATM network (AAL1), the estimated bandwidth requirements are:

- Subnet A WAN bandwidth with ATM overhead
  = 112.32 × 1.2
  = 134.78 Kbps.
- Subnet B WAN bandwidth with ATM overhead
  = 187.2 × 1.2
  = 224.64 Kbps
- Subnet C WAN bandwidth with ATM overhead
  = 37.44 × 1.2
  = 44.93 Kbps

Note: Bandwidth values can vary slightly depending on the transport type.

—————————— ***End of Example*** ——————————

VoIP bandwidth management zones

Each Internet Telephone and Voice Gateway Media Card port is assigned a zone number in which it resides. The zone indicates the VoIP bandwidth management zone of the IP devices so that IP bandwidth can be managed within locations and between locations. This enables users to avoid quality degradation because of insufficient bandwidth for active connections.

For example, a branch office or telecommuter location can have more Internet Telephones than are supported by the IP link to that location (for example, 128 Kbps bandwidth with 10 Internet Telephones).

The zones are also used to determine if voice compression and silence detection is used for a connection.

Zone properties are defined in LD 117. Up to 256 zones can be configured. The Meridian 1 and Succession CSE 1000 systems use the zones for bandwidth management. New calls are blocked when the bandwidth limit is reached.

Each zone has four parameters. The prompt lists the parameters as p1, p2, p3, p4, and p5:

- p1 - The total bandwidth available for intrazone calls.
- p2 - The preferred strategy for the choice of codec for intrazone calls (that is, preserve best quality or best bandwidth).
- p3 - The total bandwidth available for interzone calls.
- p4 - The preferred strategy for the choice of the codec for interzone calls.
- p5 - The zone resource type; the type is either shared or private.

The Call Server uses the values shown in Table 36 on page 158 when calculating the bandwidth each call uses in a zone. The Call Server cannot determine whether the LAN/WAN connection is Half or Full Duplex. Therefore, the Call Server assumes the worse case, and subtracts the bandwidth consumed on a Half Duplex link by the codec and voice payload combination from the available zone bandwidth.

This should be considered when entering a zone's intra and inter bandwidth values in LD 117. If the zone has Full Duplex links, then the bandwidth entered should be doubled. For example, with a 100 BaseT Full Duplex LAN, the intra zone bandwidth can be configured to be 200000.

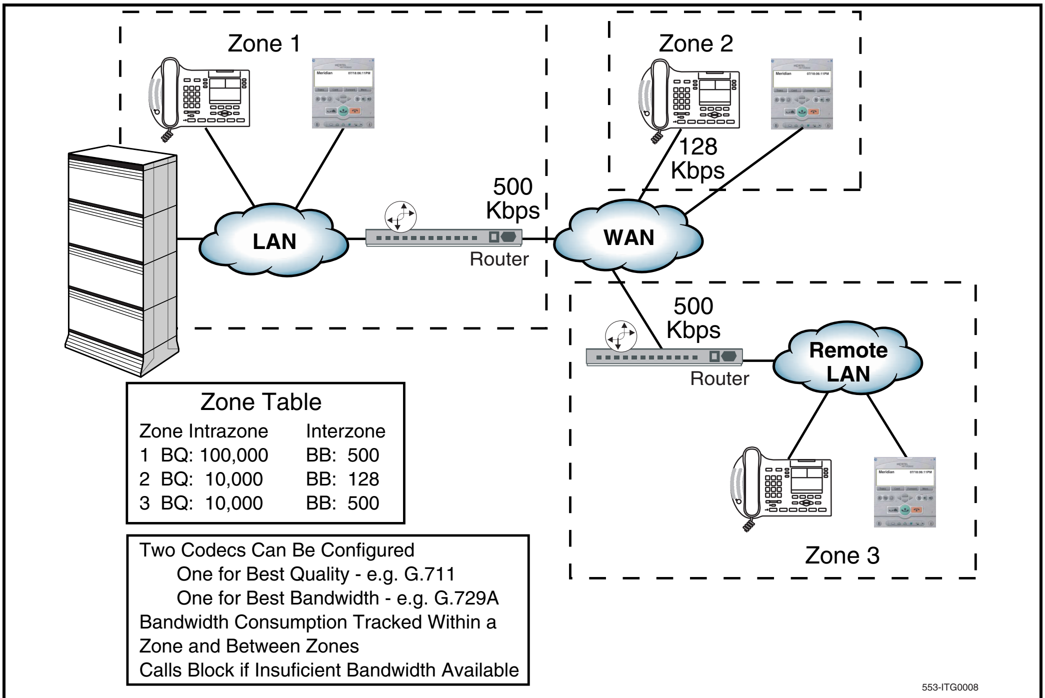
If no IP voice zones are configured, zone 0 operates as a default zone with no restrictions on bandwidth usage. If no IP voice zones are configured in LD 117, zone 0 can be configured for IPTN in LD 14, and for virtual line in LD 11 as a default zone. However, if any additional zones are required, zone 0 must be first configured in LD 117 if it is referenced by any Internet Telephone or ITG Physical TNs (IPTN). If zone 0 is not configured first, then all calls in zone 0 are labeled as soon as another zone is configured in LD 117.

> **CAUTION**
> When moving an Internet Telephone, the Administrator should check and change, if necessary, the telephone's zone assignment in LD 11. See *Software Input/Output: Administration* (553-3001-311).

> **CAUTION**
> Zone 0 must be configured in LD 117 before other zones are configured or all calls associated with zone 0 are blocked.

Figure 9 on page 166 shows an example of bandwidth management.

Figure 9
Bandwidth management example



Note: Bandwidth values given are for available bandwidth for VoIP and not for total bandwidth capacity.

Relationship between zones and subnets

Internet Telephones and Voice Gateway Media Cards gateway ports are assigned to zones based on the bandwidth management requirements of the particular installation. Devices in different subnets must traverse a router to communicate and can lie on different ends of a WAN facility. When Internet Telephones and gateway ports are in different subnets, the network facilities between them must be examined to see if it warrants placing the separated devices in different zones.

It is not necessary to always assign different zones. For instance, there can be different subnets within a LAN interconnected by router(s) with sufficient bandwidth. The Internet Telephones and gateway channels spread across them could all reside in a single zone. However, if there is a WAN facility with limited bandwidth between two subnets, the devices on the opposite ends should be placed in different zones so the bandwidth across the WAN can be managed.

Link utilization assessment

To assess the link utilization, follow the steps in Procedure 4.

Procedure 4
Assessing link utilization

1 Obtain a current topology map and link utilization report of the intranet.

2 Visually inspect the topology map to reveal which WAN links are likely to be used to deliver IP Line traffic. Alternately, use the traceroute tool (see "The following measuring tools are based on the ICMP (Internet Control Messaging Protocol):" on page 175).

3 Find out the current utilization of the WAN links. For example, the link's use can be averaged over a week, a day, or an hour.

4 Obtain the busy period (peak hour) use of the link.

5 Since WAN links are Full Duplex and data services exhibit asymmetric traffic behavior, obtain the utilization of the link representing traffic flowing in the heavier direction.

6 Assess how much spare capacity is available.

Enterprise intranets are subject to capacity planning policies that ensure that capacity usage remains below some pre-determined use level.

For example, a planning policy states that the use of a 56 Kbps link during the peak hour must not exceed 50%; for a T1 link, the threshold is higher, perhaps 80%. The carrying capacity of the 56 Kbps link would therefore be 28 Kbps, and for the T1, 1.2288 Mbps. In some organizations, the thresholds can be lower than that used in this example; in the event of link failures, there needs to be spare capacity for traffic to be re-routed.

7 The difference between the current capacity, and its allowable limit, is the available VoIP capacity.

For example, a T1 link used at 48% during the peak hour, with a planning limit of 80% has an available capacity of about 492 Kbps.

End of Procedure

Estimating network loading due to IP Line

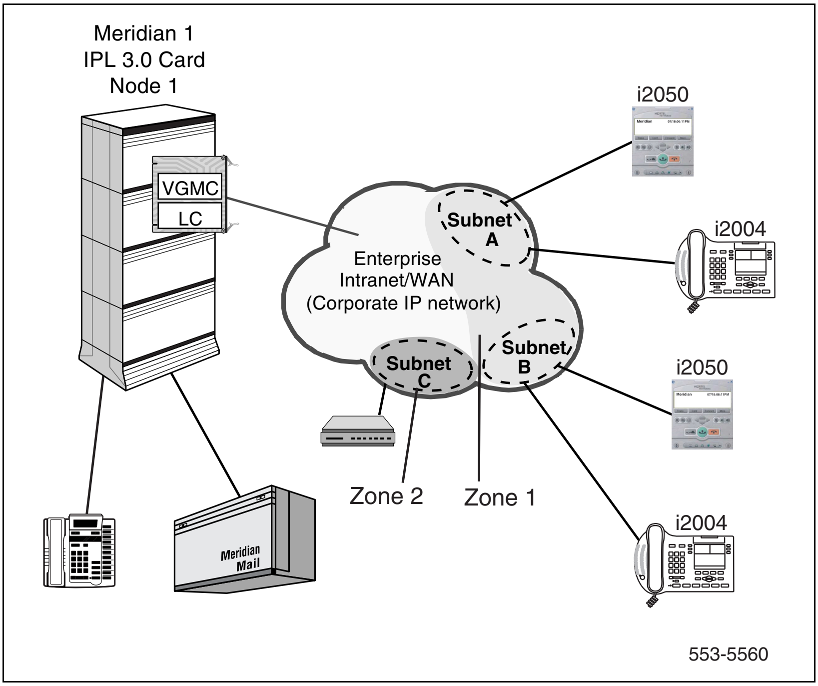
At this point, the technician has enough information to "load" the IP Line traffic on the intranet. The following example illustrates how this is done on an individual link. Not only must the IP Line traffic be taken into account but also the ITG Trunk traffic.

Example:

The intranet has a topology as shown in Figure 10 on page 169, and the technician wants to predict the amount of traffic between the IP Telephony node and corporate intranet. From the Calculate IP Line traffic requirements section (see page 155) and traceroute measurements, the traffic is collected between the IP Telephony node and subnet A, the IP Telephony node and subnet B, and the IP Telephony node and Router/Server C.

To complete this example, the traffic flow from the IP Telephony node to all routes needs to be totaled to determine the load to the link (TLAN).

Figure 10
An IP Line intranet with subnetworks



Decision: Is there sufficient capacity?

A link is defined as the route between the IP Telephony node and a subnet. Table 37 organizes the computations for each link, so that the available link capacity can be compared against the additional Voice Gateway Media Card load. For example, on the link from the IP Telephony Node to Subnet C, there is plenty of available capacity (568 Kbps) to accommodate the additional 24 Kbps of Voice Gateway Media Card traffic.

Table 37
Link Utilization Summary Example

Link		Utilization (%)		Available capacity (Kbps)	Incremental Voice Gateway Media Card Traffic (Kbps)	Sufficient capacity?
End-points	Capacity (Kbps)	Threshold	Used			
IPLine_Node1 - SubnetA	1536	80	75	76.8	72.5	Yes
IPLine_Node1 - SubnetB	1536	80	50	460.8	120.9	Yes
IPLine_Node1 - SubnetC	1536	80	48	492	24.2	Yes

Some network management systems have network planning modules that compute network flows in the manner just described. These modules provide detailed and accurate analysis as they take into account actual node, link, and routing information. They also help the technician assess the network resilience by conducting link and node failure analysis. By simulating failures, re-loading the network, and re-computing routes, the modules indicate where the network can run out of capacity during failures.

Insufficient link capacity

If there is insufficient link capacity, consider upgrading the link's bandwidth. RTP header compression can be implemented on the WAN router if it is a narrow bandwidth WAN link (less than 1.5 Mbps).

Set service parameters

Quality of Service (QoS) mechanism

The QoS requested from the IP network is controlled by the DiffServ Code Point (DSCP). QoS is controlled by setting the DSCP field in the IP header for both the Voice Gateway Media Card and the Internet Telephone. Individual values are configurable for the voice and control DSCP values and can be configured to a number between 0 and 63 inclusive. DSCP values control per hop behavior for packet forwarding for the router. The values are set once for each system and apply to all packets sent by the Voice Gateway Media Card and the Internet Telephone.

If DiffServ is implemented on the network, ask the network administrator for the default values that are used in the system. The recommended configuration values are:

- voice DSCP: 46 - Expedited Forwarding (EF) per hop behavior
- control DSCP: 40 - Class Selector 5 (CS5)

Note: OTM and Element Management have 46 and 40 as the default values.

In some cases, the IP Network Administrator can set the DiffServ field at the edge of the QoS-controlled network by routers at the network edge. DiffServ can be set based on source or destination address, or port number. The Voice Gateway Media Card and Internet Telephone can be configured to have RTP voice UDP port numbers in a specific range.

Voice Gateway Media Card and Internet Telephone port numbers

Table 38 lists the UDP ports used for IP Line to Internet Telephone communications.

Table 38
UDP ports used for IP Line to Internet Telephone communications (Part 1 of 2)

Port usage	Port number mapping
Signaling (UNIStim over RUDP link)	IP Line port 5100 to Internet Telephone port 5000 ***Note:*** Port 5000 is fixed by the Internet Telephone.
Voice (Media)	RTP: • ITG-P Line Card IP Line port 5200 - 5246 (even numbers) to Internet Telephone port 5200 • Succession Media Card IP Line port 5200 - 5262 (even numbers) to Internet Telephone port 5200 ***Note:*** The OTM user interface enables setting a "Voice Port" value; this sets both the Internet Telephone RTP port and the starting port for the IP Line gateway's RTP port range. 5200 is the default. The Internet Telephone uses port 5200 while the IP Line gateway channels [0-23] use the even port numbers in the range [5200 - 5246]. RTCP: • ITG-P Line Card IP Line port 5201 - 5247 (odd numbers) to Internet Telephone port 5201 • Succession Media Card IP Line port 5201 - 5263 (odd numbers) to Internet Telephone port 5201 ***Note:*** The RTCP port numbering is based on each channel's RTP port + 1. Therefore, the RTCP port range is dependent on the configuration for RTP port.

Table 38
UDP ports used for IP Line to Internet Telephone communications (Part 2 of 2)

Port usage	Port number mapping
Registration	IP Line ports 4100 and 7300 to Internet Telephone port 5000
i2002/i2004 Internet Telephone firmware download	TFTP standard port 69

Table 39 lists the other UDP ports used by the IP Line.

Table 39
Other UDP ports used by the IP Line

Port usage	Port number mapping
Bidirectional TPS to TPS signaling (intercard)	16543
SNTP signaling	20000 + IP Telephony node number
BOOTP server on Leader	67 (standard)
BOOTP client on Followers	68 (standard)
SNMP on ELAN interface	161 (standard)
RUDP signaling with Meridian 1 core CPU on ELAN interface	15000 15001

Measure intranet Quality of Service

Utilization of the existing data network must be assessed to determine the quality of voice services it can support.

End-to-end delay and error characteristics of the intranet must be measured so that the technician can set realistic QoS expectations for intranet voice services.

> **WARNING**
> Network designers must be aware of traffic calling patterns between any combination of Internet Telephones and gateway channels, and must plan the capacity of connecting elements to handle the expected traffic.

The use of measuring tools requires a source node and a destination node. The source node can be a "PING" (see page 175) host on a LAN segment attached to the router intended to support the node. The destination node can be a remote subnet. The requirement is briefly described as follows.

> ***Note:*** Ensure that the ITG network DiffServ bytes are set to their intended operational values before taking measurements.

Criteria

- **End-to-end packet delay:** Packet delay is the point-to-point, one-way delay between the time a packet is sent to the time it is received at the remote end. It is comprised of delays at the Voice Gateway Media Card, Internet Telephone, and the IP network. To minimize delays, the IP Telephony node and Internet Telephone must be located to minimize the number of hops to the network backbone or WAN.

  Note: To ensure good voice quality, an end-to-end delay of <= 50 ms is recommended on the IP network. This does not include the built-in delay of the Voice Gateway Media Card and Internet Telephone.

- **End-to-end packet loss:** Packet loss is the percentage of packets sent that do not arrive at their destination. Transmission equipment problems, packet delay, and network congestion cause packet loss. In voice conversation, packet loss appears as gaps in the conversation. Sporadic loss of a few packets can be more tolerable than infrequent loss of a large number of packets clustered together.

  Note: For high-quality voice transmission, the long-term average packet loss between the Internet Telephones and the Voice Gateway Media Card TLAN interface must be < 1%, and the short-term packet loss must not exceed 5% in any 10-second interval.

  Packet loss on the ELAN interface can cause:

  — communication problems between the Call Server and the Voice Gateway Media Cards

  — lost SNMP alarms

  — incorrect status information on the OTM console

  — other signaling related problems

  Note: Since the ELAN network is a Layer 2 Switched LAN, the packet loss must be zero. If packet loss is experienced, its source must be investigated and eliminated. For reliable signaling communication on the ELAN interface, the packet loss must be < 1%.

The following measuring tools are based on the ICMP (Internet Control Messaging Protocol):

- PING (sends ICMP echo requests)
- Traceroute (sends packets to unequipped port numbers and processes to create ICMP destination unavailable messages).

Both PING and traceroute are basic measuring tools that can be used to assess the IP Line network. They are standard utilities that come with most commercial operating systems. PING is used to measure the round-trip delay of a packet and the percentage of packet loss. Traceroute breaks down delay segments of a source-destination pair and any hops in-between to accumulate measurements.

There are several third-party applications that perform data collection similar to PING and traceroute. In addition, these programs analyze data and plot performance charts. The use of PING and traceroute to collect data for manual analysis is labor intensive; however, they provide information as useful as the more sophisticated applications.

The following analysis use PING/traceroute data for discussion, although it is likely in most situations a third-party application is used.

Destination Types

To a remote subnet

This configuration involves an intranet subnet that is attached to a number of Internet Telephones, that becomes an intermediate hop in the path delivering voice packets between the Internet Telephone and the IP Line network. Collect the delay measurement between the PING host and the subnet server.

Measuring end-to-end network delay

The basic tool used in IP Line networks to measure end-to-end network delay is the PING program. PING takes a delay sample by sending an ICMP packet from the host of the PING program to a destination server, and waits for the packet to make a round trip.

To ensure the delay sample results are representative of the IPLine_Node1:

- **a** Attach the PING host to a “healthy” LAN segment.
- **b** Attach the LAN segment to the router intended to support the IP Telephony node.
- **c** Choose a destination host by following the same critical guidelines as for the source host.

The size of the PING packets can be any number; the default is 60 bytes.

Sample PING output:

```
IPLine_Node1% PING -s subnetA 60
PING subnetA (10.3.2.7): 60 data bytes
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=97ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=100ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=102ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=97ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=95ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=94ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=112ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=97ms
^?
--- IPLine_Node1 PING Statistics ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip (ms) min/avg/max = 94/96/112
```

Note: PING results can vary.

Assessment of sample PING output

Note: The round-trip time (rtt) is indicated by the time field.

The rtt from the PING output varies. It is from repeated sampling of rtt that a delay characteristic of the intranet can be obtained. To obtain a delay distribution, the PING tool can be embedded in a script that controls the frequency of the PING probes, timestamps and stores the samples in a raw data file. The file can then be analyzed later using a spreadsheet or another application. The technician can also check if the intranet's network management software has any delay measurement modules that can obtain a delay distribution for a specific route.

Delay characteristics vary depending on the site pair and the time-of-day. The site pair is defined as the measurement between the host IP Line and the remote subnet (for example, IP Line to subnet A in Figure 10 on page 169). The assessment of the intranet must include taking delay measurements for each IP Line site pair. If there is a significant variation of traffic on the intranet, include PING samples during the intranet's peak hour. For a complete assessment of the intranet's delay characteristics, obtain PING measurements over a period of at least a week.

Measuring end-to-end packet loss

The PING program also reports whether the ICMP packet successfully completed its round trip. Use the same PING host setup to measure end-to-end error, and in making delay measurement, use the same packet size parameter.

Multiple PING samples must be used when sampling for error rate. Packet loss rate (PLR) is the error rate statistic collected by multiple PING samples. To be statistically significant, at least 300 samples must be used. Obtaining an error distribution requires running PING over a greater period of time.

Recording routes

The traceroute tool records routing information for all source-destination pairs as part of the network assessment. An example of the traceroute output is shown below:

```
ipline_node1% traceroute subnetA
traceroute to subnetA 10.3.2.7, 30 hops max, 32 byte packets
1    r6 (10.8.0.1) 1 ms  1 ms  1 ms
2    r5 (10.18.0.2) 42 ms  44 ms  38 ms
3    r4 (10.28.0.3) 78 ms  70 ms  81 ms
4    r1 (10.3.0.1) 92 ms  90 ms  101 ms
5    subnetA (10.3.2.7) 94 ms  97 ms  95 ms
```

The traceroute program is also used to verify whether routing in the intranet is symmetric or not for each of the source-destination pairs. This is done using

the -g loose source routing option, as illustrated in the following command syntax:

```
ipline_node1% traceroute -g subnetA ipline_node1
```

Adjusting PING measurements

One-way and roundtrip

The PING statistics are based on round-trip measurements, while the QoS metrics in the Transmission Rating model are one-way. Divide the delay and packet error PING statistics in half to ensure the comparison is valid.

Adjustment due to IP Line processing

The PING measurements are taken from PING host to PING host. The Transmission Rating QoS metrics are from end-user to end-user, and include components outside the intranet. The PING statistic for delay needs to be further modified by adding 93ms to account for the processing and jitter buffer delay of the nodes.

> ***Note:*** No adjustment needs to be made for error rates.

If the intranet measurement barely meets the round-trip QoS objectives, the technician must be aware of the possibility that the one-way QoS is not being met in one of the directions of flow. This can apply even if the flow is on a symmetric route due to asymmetric behavior of data processing services.

Late packets

Packets that arrive outside the window allowed by the jitter buffer are discarded by the IP Line. To determine which PING samples to ignore, calculate the average one-way delay based on all the samples.

To calculate late packets, double the value of the nominal jitter buffer setting. For example, assume:

- the average one-way delay is 50 msec
- the jitter buffer is set to a nominal (or average) value of 40 msec
- then the maximum value is 2 x 40 + 50 = 130 msec

Therefore, any packet with a one-way delay of greater than 130 msec is late, and must be added to the total number of packets lost.

Estimate Voice Quality

The perceived quality of a telephone call is dependent on many factors, such as codec characteristics, end-to-end delay, packet loss, and the perception of the individual listener.

The E-Model Transmission Planning Tool is a model used to produce a quantifiable measure of voice quality based on relevant factors. Refer to two ITU-T recommendations (ITU-T E.107 and E.108) for more information on the E-Model and its application.

A simplified version of the E-Model is applied to the Internet Telephone to provide an estimate of the voice quality that the user can expect based on various configuration choices and network performance metrics.

The simplified E-Model is given below:

R = 94 - lc - ld - lp

where:
lc = codec impairment (see Table 40 on page 181)

ld = delay impairment (see Table 41 on page 181)

lp = packet loss impairment (see Table 42 on page 182)

Note: This model already takes into account some characteristics of the Internet Telephone, and therefore the impairment factors are not identical to those shown in the ITU-T standards.

Refer to Table 43 on page 182 for the translation of R values into user satisfaction levels.

Table 40
Impairment factors of codecs

Codec	Codec Impairment (Ic) (msec frames)
G.711	0
G.729A/AB	11 - 20 or 30
G.729A/AB	16 - 40 or 50
G.723.1 (5.3 Kbps)	19
G.723.1 (6.3 Kbps)	15

Table 41
Impairment factors due to network delay

Network delay* (msec)	Delay Impairment (Id)
0 -49	0
50 - 99	5
100 -149	10
150 - 199	15
200 - 249	20
250 - 299	25
* Network delay is the average one-way network delay plus jitter.	

Table 42
Impairment factors due to packet loss

Packet loss (%)	Packet Lose Impairment (Ip)
0	0
1	4
2	8
4	15
8	25

Table 43
R value translation

R Value (lower limit)	MOS	User Satisfaction
90	4.5	Very satisfied
80	4.0	Satisfied
70	3.5	Some users dissatisfied
60	3.0	Many users dissatisfied
50	2.5	Nearly all users dissatisfied
0	1	Not recommended

Sample scenarios

Scenario 1

A local LAN has the following characteristics:

- G.711 codec
- 20 msec network delay
- 0.5% packet loss

To calculate R = 94 - lc - ld - lp, use Table 40, Table 41, and Table 42:

- G.711 codec: lc = 0
- 20 msec network delay: ld = 0
- 0.5% packet loss: lp = 2

Then:

R = 94 - 0 - 0 - 2

R = 92

Using Table 43 on page 182, a value of 92 means the users are very satisfied.

Scenario 2

A campus network has the following characteristics:

- G.711 codec
- 50 msecs delay
- 1.0% packet loss

To calculate R = 94 - lc - ld - lp, use Table 40, Table 41, and Table 42:

- G.711 codec: lc = 0
- 20 msec network delay: ld = 5
- 0.5% packet loss: lp = 4

Then:

R = 94 - 0 - 5 - 4

R = 85

Using Table 43 on page 182, a value of 85 means the users are satisfied.

Scenario 3

A WAN has the following characteristics:

- G.729 codec
- 30 msec network delay
- 2% packet loss.

To calculate R = 94 - lc - ld - lp, use Table 40, Table 41, and Table 42:

- G.711 codec: lc = 11
- 20 msec network delay: ld = 5
- 0.5% packet loss: lp = 8

Then:

R = 94 - 11 - 5 - 8

R = 70

Using Table 43 on page 182, a value of 70 means some users are dissatisfied.

DiffServ

The Differentiated Service (DiffServ) determines the priority of the packets in the IP network. The value entered depends on the equipment in the data network. The DiffServ applies to all cards in the node and also applies to any Internet Telephones that register with this node.

Individual values are configurable for the voice and control DiffServ Code Point (DSCP) values and can be configured to a number between 0 and 63 inclusive using OTM 2.0.

The values are set once for each system and apply to all packets sent by the Voice Gateway Media Card and the Internet Telephone.

If DiffServ is implemented on the network, ask the network administrator for the default values that are used in the system. The recommended configuration values are:

- voice DSCP: 46 - Expedited Forwarding (EF)
- control DSCP: 40 - Class Selector 5 (CS5)

> ***Note:*** OTM and Element Management has 46 and 40 as the default values.

Loss and Level Plan

The Voice Gateway Media Card ships with a predefined loss and level plan. The loss and level plan determines various parameters, such as transmission gain, that vary from country to country. The default loss and level plan is for the United States. The values are stored in a file on the OTM PC. You can select other countries when you configure the DSP Profile settings in OTM's ITG Line 3.0 application or the Loss Plan settings in Element Management.

> ***Note:*** A dynamic loss plan has been implemented on the Succession CSE 000 Rel 2.0 system. It uses PDCA Table 15 in LD 73 to define the gateway loss value per endpoint connection type and adjusts the Voice Gateway Media Card gateway channel's loss for each call by sending pad values to the card. The default values in the system are for the North American loss plan. Installation of the Succession CSE 000 Rel 2.0

system in any other country requires setting the pad values in Table 15 to that country's loss plan. See the section on Transmission Parameters in Planning and Engineering Guidelines (553-3023-102) for details.

Echo canceller

OTM supports echo canceller tail lengths of 8, 16, and 32 msec. The default in OTM is the maximum of 32 msec. Element Management supports echo canceller tail lengths of 0, 64, and 128 (default) msec. It is recommended that the maximum echo canceller tail length is used. Never reduce the echo canceller tail delay value unless directed by Nortel Networks Field Support.

OTM's scaling process

The IP Line loadware contains an enhanced echo canceller. The new echo canceller has improved echo cancellation algorithms and supports tail lengths up to 128 msec. OTM 1.0.15 does not offer the enhanced tail length values in the echo canceller tail pull down menu. Because the IP Line loadware can be used with any supported version of the OTM product, it scales the configured tail length, if necessary, so that the maximum tail length is achieved. The scaling provides the following echo cancelling tail lengths:

8 -> 32 msec
16 -> 64 msec
32 -> 128 msec

The maximum tail length is the recommended value. Selecting the OTM default of 32 msec yields the desired maximum tail length of 128 msec.

An update to OTM changes the echo canceller tail configuration pull down list to the values 64 and 128. When used with the IP Line loadware, the application no longer needs to scale the configured value. The configured value matches the tail length used by the echo canceller.

> ***Note:*** If the OTM version 2.0 is used with an ITG Line 2.0 loadware version, such as ITG Line 2.01.53, selecting 64 or 128 msecs sets the echo tail length to 32 msec.

Reducing delays

The link delay is the time it takes for a voice packet to be queued on the transmission buffer of a link until it is received at the next hop router. Link delay can be reduced by:

- Upgrading link capacity. This reduces the serialization delay of the packet, but also reduces the utilization of the link and the queueing delay. Before upgrading a link, the technician must check both routers connected to the link to be upgraded and ensure compliance with router configuration guidelines.
- Implementing a priority queueing discipline.

To determine the links for upgrading, list all the intranet links used to support the IP Line traffic. This can be derived from the traceroute output for each site pair. Use the intranet link utilization report and note the highest used links and the slowest links. Estimate the link delay of suspect links using the traceroute results.

Example: A 256 Kbps link from router1 to router 2 has a high utilization. The following is a traceroute output that traverses this link:

```
IPLine_Node1% traceroute SubnetA
traceroute to SubnetA (10.3.2.7), 30 hops max, 32 byte packets
    router1 (10.8.0.1) 1 ms 1 ms  1 ms
    router2 (10.18.0.2) 42 ms  44 ms  38 ms
    router3 (10.28.0.3) 78 ms  70 ms  81 ms
    router4 (10.3.0.1) 92 ms  90 ms  101 ms
    SubnetA (10.3.2.7) 94 ms  97 ms  95 ms
```

The average rtt time on the example link is about 40 ms; the one-way link delay is about 20 ms, of which the circuit transmission and serialization delay are just a few milliseconds. Most of this link's delay is due to queueing.

Reducing hop count

The IP Telephony nodes must be connected to the intranet to minimize the number of router hops between the Voice Gateway Media Card and the Internet Telephone. This reduces the fixed and variable IP packet delay, and improves the Voice over IP Quality of Service. It is recommended that no more than one card use a particular 10BaseT LAN collision domain.

> ***Note:*** In a passive Ethernet hub, all ports on the hub share one 10Mbps collision domain; in a switched Ethernet hub, each port has its own collision domain. Hubs should not be used anywhere in the network path between the internet telephone and VGMC TLAN interface. A switched network is recommended

The IP Telephony node and the TLAN router should be placed as close to the WAN backbone as possible to:

- Minimize the number of router hops.
- Segregate constant bit-rate VoIP traffic from bursty LAN traffic.
- Simplify the end-to-end QoS engineering for packet delay, jitter, and packet loss.

If an access router separates the IP Telephony node from the WAN router, there must be a high-speed link (for example, Fast Ethernet, FDDI, SONET, OC-3c, ATM STS-3c) between the access router and the WAN backbone router.

Reducing packet errors

Packet errors in intranets are generally correlated with congestion somewhere in the network. Bottleneck links occur where the packet errors are high because packets get dropped when they arrive faster than the link can transmit them. When highly used links are upgraded, the sources of packet errors on a particular flow must be removed. A reduction in hop count also reduces the opportunities for routers and links to drop packets.

Other causes of packet errors, not related to queueing delay:

- **Poor link quality–**the underlying circuit has transmission problems, high line error rates, or subject to frequent outages. The circuit is provisioned on top of other services, such as X.25, frame relay, or ATM. Check with the service provider for resolution.
- **Overloaded CPU–**this is another commonly-monitored statistic collected by network management systems. If a router is overloaded, it means that the router is constantly performing processing-intensive tasks, which impedes the router from forwarding packets. Find out what the threshold CPU utilization level is, and check if any suspect router conforms to the threshold. The router has to be re-configured or upgraded.
- **Saturation–**routers can also be overworked when there are too many high capacity and high traffic links configured on it. Ensure that routers are dimensioned according to vendor guidelines.
- **LAN saturation–**packets are dropped on under-engineered or faulty LAN segments.
- **Jitter buffer too small–**packets that arrive at the destination ITG, but are too late to be placed in the jitter buffer, are essentially loss packets.

Adjusting jitter buffer size

The jitter buffer parameters directly affect the end-to-end delay. Lowering the voice playout settings decreases one-way delay, but there is less waiting time for voice packets that arrive late.

The jitter buffer setting is configured on the voice gateway channels of the Voice Gateway Media Card and are sent out to the Internet Telephones. The jitter buffer size is set when you configure the DSP Profiles:

- in the OTM ITG Line 3.0 application (see Figure 40 on page 285), or
- in the selected codec in Element Management (see Figure 66 on page 349)

The jitter buffer is statically configured and is the same for all devices in the network. The jitter buffer size range is 0-200 milliseconds. The default jitter buffer value is 50 milliseconds. However, the jitter buffer setting that is used on the Voice Gateway Media Card is a multiple of the codec frame size. The setting is automatically adjusted to be greater than or equal to the jitter buffer value set in the DSP Profile tab. As each call is set up, the jitter buffer for each device is set to the nearest whole number increment of the selected codec frame size.

For example, if the jitter buffer is configured as the default 50 msec in the DSP Profiles, but a 20 msec codec is used, the jitter buffer is set to 60 msec, which is the nearest whole number increment.

> 50 msec / 20 msec = 2.5
> 2.5 rounded up to the nearest whole number increment is 3.
> 3 x 20 msec = 60 msec

If the jitter buffer is configured as zero, the depth of the jitter buffer is set to the smallest value the device can support. In practice, the optimum depth of the jitter queue is different for each call. For telephones that are on a local LAN connection, a short jitter queue is desirable to minimize delay. For telephones that are several router hops away, a longer jitter queue is required.

Lowering the jitter buffer size decreases the one-way delay of voice packets. If the setting for the jitter buffer size is too small, packets are discarded unnecessarily. Discarded packets result in poorer speech quality and can be heard as clicks or choppy speech.

If the technician decides to discard packets, to downsize the jitter buffer, the technician must do the following:

- **Check the delay variation statistics.**

  Obtain the one-way delay distributions originating from all source IP Line sites.

- **Compute the standard deviation of one-way delay for every flow.**

  Some traffic sources with few hop counts yield small delay variations, but it is the flows that produce great delay variations that should be used to determine whether it is acceptable to resize the jitter buffer.

- **Compute the standard deviation (σ) of one-way delay for that flow.**

  Do not set the set the jitter buffer size smaller than 2s.

Codec selection

To ensure optimal voice quality, minimize the number of compression and decompression stages and wherever bandwidth permits, use G.711 codec.

There is a potential to degrade the voice quality if codecs are cascaded. This can occur when there are multiple compression and decompression stages on a voice call. The more IP links used in a call, the more delay is added, and the greater the impact on the voice quality.

The following is a list of applications and devices that can impact voice quality, if you use a compression codec such as G.729A:

- Voice mail, such as Nortel Networks CallPilot**,** introduces another stage of compression and decompression.
- Conferences can double the number of IP links.
- ITG Trunks can add additional stages of compression and decompression.

Post-installation network measurements

The design process is continual, even after implementation of the ITG network and commissioning of voice services over the network. Network changes – in ITG traffic, general intranet traffic patterns, network policies, network topology, user expectations, and networking technology – can render a design obsolete or non-compliant with QoS objectives. The design needs to be reviewed periodically against prevailing network conditions and traffic patterns.

It is assumed that the customer's organization already has processes to monitor, analyze, and re-design both the Meridian 1 and Succession CSE 1000 network and the corporate intranet to maintain internal QoS standards. When operating an ITG network, additional processes must be developed to:

- collect, analyze, and forecast ITG traffic patterns

- monitor Operational Measurements (see below)
- implement changes in the ITG and intranet when planning thresholds are reached

By establishing these new processes, the ITG network can be managed to ensure that desired QoS objectives are met.

ITG Operational Measurement (OM)

The Voice Gateway Media Card collects Operational Measurements from the Internet Telephones and DSP channels and saves the information to a log file every 60 minutes. The Operational Measurements include:

- Internet Telephone Registration Attempted Count
- Internet Telephone Registration Confirmed Count
- Internet Telephone Unregistration Count
- Internet Telephone Audio Stream Set Up Count
- Internet Telephone Average Jitter (msec)
- Internet Telephone Maximum Jitter (msec)
- Internet Telephone Packets Lost/Late (%)
- Internet Telephone Total Voice Time (minutes and seconds)
- Gateway Channel Audio Stream Set Up Count
- Gateway Channel Average Jitter (msec)
- Gateway Channel Maximum Jitter (msec)
- Gateway Channel Packets Lost/Late (%)
- Gateway Channel Total Voice Time (minutes and seconds)

OM Report description

The OM log file is a comma-separated (.csv) file stored on the OTM server. Using OTM you can run an adhoc report or schedule a regular report. A new file is created for each month of the year in which OM data is collected. It can be read directly or imported to a spreadsheet application for post-processing and report generation. Collect these OM reports and store them for analysis. At the end of each month, identify the hours with the highest packet lost/late statistics and standard deviation statistics generated. Compare the data to target network QoS objectives.

Declines in QoS can be observed through the comparison of QoS between last period and current period. A consistent inferior measurement of QoS compared with the objective triggers an alarm. The customer must take steps to strengthen the performance of the route.The card creates a new log file each day. Files are automatically deleted after seven days.

IP Line ELAN and TLAN configuration

A subnet is defined as a remote network serving a collection of Internet Telephones, which is represented by a server or router communicating with the ITG processor for VoIP service (see Figure 10 on page 169).

General requirements

The general requirements are as follows:

- no foreign broadcast coming from other subnets
- no BootP relay agent requirement (only on ELAN router interface)
- no Network Address Translation (NAT) between Internet Telephone and IP Telephony node
- the TLAN cable between the ITG-P Line Card and the Layer 2 switch must be 50 meters or less
- disable spanning tree on the Layer 2 switch ports connected to the ELAN and TLAN ports of the Meridian 1 and Succession CSE 1000 components

Separate subnet configuration

Each Voice Gateway Media Card has two Ethernet ports, one for the Telephony LAN (TLAN) and one for the Embedded LAN (ELAN). The advantages of this configuration are:

- optimization of VoIP performance on the LAN segment by segregating it from ELAN traffic and connecting the TLAN as close as possible to the WAN router.
- making the amount of traffic on the TLAN more predictable for QoS engineering.
- enhanced network access security when the ELAN and customer's enterprise network are separate or connected through a fire-wall router:

— enables placement of the modem router on the isolated ELAN, protecting the customer's enterprise network from unauthorized modem router accesses

— protects the Meridian 1/Succession CSE 1000 ELAN from unauthorized access from the customer's enterprise network

CAUTION
Due to backwards compatibility, the user interface permits you to choose whether to use separate subnets. It is, however, mandatory to use separate subnets.

ELAN/TLAN Half and Full Duplex operation

The ELAN on the Voice Gateway Media Card operates at Half Duplex only and is limited to 10BaseT operation due to filtering on the Meridian 1 Option 11C back planes.

The TLAN on Voice Gateway Media Card operates at Half Duplex or Full Duplex and can run at 10BaseT or 100BaseT.

It is recommended that any network equipment connected to the ELAN or TLAN be set to Auto Sense / Auto Negotiate for correct operation. Although Full Duplex is preferred, it is not required. For example, for the IP Line application, Half Duplex has ample bandwidth for a Voice Gateway Media Card even with 24 busy channels, VAD disabled, and G.711 codec with 10ms voice range.

Mismatches can occur if devices are hard configured for speed and duplex mode. Every device and port must be correctly configured to avoid duplex mismatch problems that typically exhibit as lost packets and CRC errors. The Voice Gateway Media Card cannot be set for 100BaseT/Full Duplex operation, and as a result the card's TLAN operates in Auto Negotiate mode. Duplex mismatches and lost packets occur if the TLAN interface is not configured properly.

CAUTION
Duplex mismatches occur in the LAN environment when one side is set to Auto Negotiate and the other is hard configured.

The Auto Negotiate side adapts only to the speed setting of the fixed side. For duplex operations, the Auto Negotiate side sets itself to Half Duplex mode. If the forced side is Full Duplex, a duplex mismatch occurs.

Subnet configuration for TLAN and ELAN ports

Single subnet configuration implies the configuration and use of just one Ethernet interface, namely the ELAN interface, over which all voice and management traffic is routed. Single subnet configuration can also mean configuring both the TLAN and ELAN interfaces to be in the same subnet. Neither configuration is supported. The configuration of the ELAN and TLAN must be done such that both interfaces are used and the assigned IP addresses are in different subnets.

Separate or dual subnet configuration implies the configuration of both the TLAN and ELAN interfaces. All management traffic is routed over the ELAN, while all telephony traffic is routed over the TLAN. The ELAN connection is to a 10BaseT hub or switch, while the TLAN is connected to a 10/100BaseT switch.

For dual subnet configuration, the TLAN and ELAN subnets must not overlap. For example, the following configuration is not valid, as the TLAN and ELAN subnets overlap.

ELAN IP	10.0.0.136
ELAN Gateway	10.0.0.129
ELAN Subnet Mask	255.255.255.224
TLAN Node IP	10.0.0.56
TLAN Card IP	10.0.0.57
TLAN Gateway	10.0.0.1
TLAN Subnet Mask	255.255.255.0

The ELAN range of addresses, 10.0.0.129 to10.0.0.160, overlaps with the TLAN range of addresses, 10.0.0.1 to 10.0.0.255. This fails to keep with IP addressing practices, as it is equally valid to route to IP packets over either the TLAN or ELAN interface and the resulting behavior from such a setup is undetermined.

A better way to split these IP addresses is:

ELAN IP	10.0.0.136
ELAN Gateway	10.0.0.129
ELAN Subnet Mask	255.255.255.224
TLAN Node IP	10.0.0.56
TLAN Card IP	10.0.0.57
TLAN Gateway	10.0.0.1
TLAN Subnet Mask	255.255.255.128

In this example:

- TLAN IP addresses are in the range of 10.0.0.1 to 10.0.0.127
- ELAN IP addresses are in a separate subnet of 10.0.0129 to 10.0.0.160

This satisfies the IP addressing practice of engineering the network such that subnets do not overlap. However, this results in a smaller subnet for the TLAN address.

Spanning Tree Option on Layer 2 switches

Nortel Networks recommends disabling the spanning tree option on the Layer 2 switch ports that connect to the Meridian 1 and Succession CSE 1000 system's TLAN and ELAN interfaces.

This option is "enabled" by default on most Layer 2 switches. If the option is left enabled, the subsequent spanning tree discovery algorithm initiated when a device connected to a port is reset, rebooted, or unplugged/plugged-in, can interfere with the Master Election Process of the Meridian 1 and Succession CSE 1000 system devices. In most cases the Master Election Process recovers from this after a slight delay. However, to reduce the potential of unforeseen complications in this scenario it is recommended that the spanning tree option on these ports be disabled.

LAN Device Interface Names

The devices in the system have different Device Interface Names depending on whether is it is on the TLAN or on the ELAN. Table 44 on page 198 shows the Device Interface Name for the Succession Media Card, ITG-P Line Card, and the Signaling Server.

Table 44
LAN Device Interface Names

Device Type	TLAN/ELAN	LAN Device Interface Name
Succession Media Card	ELAN	ixpMac1
	TLAN	ixpMac0
ITG-P Line Card	ELAN	lnIsa0
	TLAN	lnPci1
Signaling Server	ELAN	fei0
	TLAN	fei1

Installation and Configuration Summary

Contents

This section contains information on the following topics:

Reference list

The following are references for this section:

- *Internet Terminals Description* (553-3001-217)
- *Software Input/Output: Maintenance* (553-3001-511)

Overview

This chapter provides a summary of the procedures required to install a new Meridian 1 and Succession Communication Server for Enterprise (CSE) 1000 IP Telephony node, add cards to the node, install the cards, transmit data to the cards, and install the Internet Telephones. It also includes information on what you need before beginning the installation procedures.

Be sure to read the "IP Network Engineering Guidelines" on page 133 before installing an IP Telephony node.

The follow chapter is divided into two summary sections.

- "Meridian 1 Rel 25.30 or Succession CSE 1000 Rel 1.1 systems" on page 200
- "Succession CSE 1000 Rel 2.0 systems" on page 204

Meridian 1 Rel 25.30 or Succession CSE 1000 Rel 1.1 systems

Before you begin:

1 Ensure that the system meets the following minimum requirements: Meridian 1 Release 25.30 system or Succession CSE 1000 Release 1.1 system.

2 Upgrade the Meridian 1 or Succession CSE 1000 keycode to expand the ISM system limit to support the number of Internet Telephones you plan to install. Refer to *Software Input/Output: Maintenance* (553-3001-511) to use:

- **a.** LD 22 command SLT to determine your Internet Telephone limit on the system.
- **b.** LD 143 to expand the ISM parameters (if required).

3 Verify that you have the Optivity Telephony Manager (OTM) version 2.0.

- **a.** Check the Nortel Networks Software Downloads Web site to determine the latest software version and required patches (PEPs).

Refer to Procedure 111, “Downloading files from the Nortel Networks Web site” on page 719.

b. Upgrade to the latest OTM version if necessary.

4 Create site name, system name, and customer number in the OTM Navigator. Specify the correct Meridian 1 and Succession CSE 1000 system type in order for OTM ITG IP Line 3.0 application to prompt for correct TN format.

5 Provision the IP network to support IP Telephony node and Internet Telephones.

a. Choose the Internet Telephone DHCP mode: Full, Partial, or None (static IP address). For Full DHCP mode, refer to “Configuring the DHCP server to support Full DHCP mode” on page 215.

b. Determine the Internet Telephone 10/100BaseT Ethernet LAN connection: desktop switch, or a separate cable to the equipment closet.

c. Determine TLAN, ELAN IP address and Ethernet connections from the network IP administrator. Refer to the “IP Network Engineering Guidelines” on page 133.

6 Check that the required LAN and WAN networking equipment and cables are installed. For IP networking requirements, refer to “IP Network Engineering Guidelines” on page 133.

Installation summary for Meridian 1 Rel 25.30 and Succession CSE 1000 Rel 1.1 systems

The following summary of steps can be used as a reference guide to install and configure an IP Telephony node and Voice Gateway Media Cards on Meridian 1 and Succession CSE 1000 Release 1.1 systems. This summary is intended to serve as a pointer to the more detailed procedures contained in other chapters and to provide a sequential flow to the steps involved in the overall installation procedure.

> ***Note:*** Complete all installation and configuration steps before you transmit data to the Voice Gateway Media Cards.

1 Complete the Voice Gateway Media Card installation summary sheet. Refer to Table 45 on page 209.

2 Complete the Internet Telephone configuration data summary sheet. Refer to Table 46 on page 210.

3 Install the hardware components:

- **a.** Install and cable the Voice Gateway Media Card(s). See Procedure 5 on page 230 for installing the ITG-P Line Cards and to Procedure 7 on page 236 for installing the Succession Media Card.
- **b.** Install an ITG Line-specific I/O Panel Filter Connector (Option 51C/61C/81/81C only). See Procedure 8 on page 238.
- **c.** Cable the Voice Gateway Media Card:
  - **i.** Install the ELAN, TLAN, serial interface cable for the ITG-P Line Card. See Procedure 9 on page 243.
  - **ii.** Install the Shielded 50-pin to Serial/ELAN/TLAN Adapter for the Succession Media Card. See Procedure 10 on page 246.

4 Configure IP Line data on the Meridian 1 and Succession CSE 1000:

- **a.** Configure the IP address for the Meridian 1 and Succession CSE 1000 ELAN Ethernet interface. See Procedure 11 on page 248.
- **b.** Configure VoIP bandwidth management zones. See page 249.
- **c.** Configure IP Line physical TNs. See page 253.
- **d.** Configure virtual superloops. See page 259.

- **e.** Configure Option 11C/11C-Mini mapping of virtual superloops. See page 260.
- **f.** Configure Internet Telephone Meridian 1 and Succession CSE 1000 features. See page 263.

5 Configure IP Line data using OTM:

- **a.** Manually add an IP Telephony node. See page 278.
- **b.** Configure Voice Gateway Media Care properties. See page 282.
- **c.** Configure DSP Profile data. See page 284.
- **d.** Configure SNMP traps and Card routing table entries (if required). See page 288.
- **e.** Configure Meridian 1 and Succession CSE 1000 Call Server ELAN IP (Active ELNK) address and TLAN Voice port on the Voice Gateway Media Card. See page 292.
- **f.** Configure SNMP Community Names access for security. See page 295.
- **g.** Configure access to the file server. See page 296.
- **h.** Configure 802.1Q support and NAT support. See page 298.

6 Transmit Voice Gateway Media Card configuration data from OTM to the Voice Gateway Media Cards:

- **a.** Set Leader 0 IP Address. See Procedure 24 on page 301.
- **b.** Transmit node and card properties to Leader 0. See Procedure 25 on page 303.
- **c.** Transmit card properties to all cards in the node. See Procedure 26 on page 305.

7 Upgrade card loadware and i2004 Internet Telephone firmware:

- **a.** Verify card loadware and i2004 Internet Telephone firmware release. See page 309.
- **b.** Determine latest loadware and firmware versions from Meridian 1 and Succession CSE 1000 Nortel Networks Web site. See page 309.
- **c.** Upgrade Voice Gateway Media Card loadware (if required). See Procedure 28 on page 314.
- **d.** Upgrade i2004 Internet telephone firmware (if required). See Procedure 30 on page 318.

8 Configure OTM alarm notification feature to receive IP Line SNMP traps. See Procedure 31 on page 323.

9 Assemble and install an Internet Telephone. Refer to the *Internet Terminals Description* (553-3001-217).

10 Change the default IP Line Command Line Interface (IPL>) Shell password. See Procedure 55 on page 415.

11 Configure the Internet Telephone Installer Passwords (see page 420).

- **a.** Enable and set the administrative Internet Telephone Installer Password. See Procedure 58 on page 429.
- **b.** If needed, enable and set a temporary Internet Telephone Installer Password. See Procedure 59 on page 433.

Succession CSE 1000 Rel 2.0 systems

Before you begin

1 Ensure that the system meets the following minimum requirements: Succession CSE 1000 Release 2.0

2 Upgrade the Succession CSE 1000 keycode to expand the ISM system limit to support the number of Internet Telephones you plan to install. Refer to *Software Input/Output: Maintenance* (553-3001-511) to use:

- **a.** LD 22 command SLT to determine your Internet Telephone limit on the system.
- **b.** LD 143 to expand the ISM parameters (if required).

3 Verify that you have access to the Signaling Server so Element Management can be run.

- **a.** Check the Nortel Networks Software Downloads Web site to determine the latest software version and required patches (PEPs). See Procedure 111, “Downloading files from the Nortel Networks Web site” on page 719.
- **b.** OTM 2.0 is be needed for certain IP Line 3.0 feature enhancements.

4 Ensure that browser caching is turned off so that Element Management runs properly. See “Internet Explorer browser configuration” on page 332.

5 Provision the IP network to support IP Telephony node and Internet Telephones.

a. Choose the Internet Telephone DHCP mode: Full, Partial, or None (static IP address). For Full DHCP mode, see "Configuring the DHCP server to support Full DHCP mode" on page 215.

b. Determine the Internet Telephone 10/100BaseT Ethernet LAN connection. There are two options for the connection:

   i. The connection can be a separate cable to the equipment closet.

   ii. The connection can be shared back to the closet using a desktop switch or the telephone's built-in 3-port switch.

c. Determine TLAN, ELAN IP address and Ethernet connections from the network IP administrator. See the "IP Network Engineering Guidelines" on page 133.

6 Check that the required LAN and WAN networking equipment and cables are installed. For IP networking requirements, see "IP Network Engineering Guidelines" on page 133.

Installation summary for Succession CSE 1000 Rel 2.0 systems

The following summary of steps can be used as a reference guide to install and configure an IP Telephony node and Voice Gateway Media Cards on Succession CSE 1000 Release 2.0 system. This summary is intended to serve as a pointer to the more detailed procedures contained in other chapters and to provide a sequential flow to the steps involved in the overall installation procedure.

> ***Note:*** Complete all installation and configuration steps before you transmit data to the Voice Gateway Media Cards.

1 Complete the Voice Gateway Media Card installation summary sheet. See Table 45 on page 209.

2 Complete the Internet Telephone configuration data summary sheet. See Table 46 on page 210.

3 Install the hardware components:

a. Install the Voice Gateway Media Card(s). See Procedure 5 on page 230 for installing the ITG-P Line Cards and Procedure 7 on page 236 for installing the Succession Media Card.

b. Cable the Voice Gateway Media Cards:

   i. Install the ELAN, TLAN, serial interface cable for the ITG-P Line Card. See Procedure 9 on page 243.

   ii. Install the Shielded 50-pin to Serial/ELAN/TLAN Adapter for the Succession Media Card. See Procedure 10 on page 246.

4 Configure IP Line data on the Succession CSE 1000 Release 2.0:

a. Configure the IP address for the Succession CSE 1000 Release 2.0 ELAN Ethernet interface. See Procedure 11 on page 248.

b. Configure VoIP bandwidth management zones. See page 249.

c. Configure IP Line physical TNs. See page 253.

d. Configure virtual superloops. See page 259.

e. Configure Option 11C/11C-Mini mapping of virtual superloops. See page 260.

f. Configure Internet Telephone Meridian 1 and Succession CSE 1000 features. See page 263.

5 Configure IP Line data using Element Management:

a. Manually add an IP Telephony node. See page 338.

b. Configure SNMP traps and community names access for security. See page 343.

c. Configure DSP Profile data. See page 346.

d. Configure DiffServ Codepoint data, 802.1Q support, and NAT support. See page 351.

e. Configure Succession CSE 1000 Call Server ELAN IP (Active ELNK) address, TLAN Voice port, and the routing tables on the Voice Gateway Media Card. See page 353.

f. Configure file server access. See page 358.

g. Configure the loss plan. See page 360.

h. Configure Voice Gateway Media Care properties. See page 361.

6 Submit and transfer the node information to the Call Server. See page 364.

7 Transmit Voice Gateway Media Card configuration data the Voice Gateway Media Cards:

- **a.** Set Leader IP Address. See Procedure 43 on page 369.
- **b.** Transmit node and card properties to Leader. See Procedure 44 on page 372.

8 Upgrade card loadware and i2004 Internet Telephone firmware:

- **a.** Verify card loadware. See page 381.
- **b.** Verify card firmware release. See page 383.
- **c.** Download loadware and firmware files from the Nortel Networks Web site. See page 386.
- **d.** Upload the loadware and firmware files to the file server. See page 387.
- **e.** Upgrade the loadware on the Voice Gateway Media Card. See page 389.
- **f.** Reboot the card. See page 393.
- **g.** Upgrade the firmware on the card. See page 394.

9 Configure OTM alarm notification feature to receive IP Line SNMP traps. See Procedure 31 on page 323.

10 Assemble and install an Internet Telephone. Refer to the *Internet Terminals Description* (553-3001-217).

11 Change the default IP Line Command Line Interface (IPL>) Shell password. See Procedure 55 on page 415.

12 Configure the Internet Telephone Installer Passwords (see page 420).

- **a.** Enable and set the administrative Internet Telephone Installer Password. See Procedure 58 on page 429.
- **b.** If needed, enable and set a temporary Internet Telephone Installer Password. See Procedure 59 on page 433.

Voice Gateway Media Card installation summary sheet

Nortel Networks recommends that you complete a Voice Gateway Media Card installation summary sheet (Table 45 on page 209) as you unpack, inventory, and provision the cards. IP address information is normally supplied by the your IP Network Administrator.

To complete the installation summary sheet, you need to know:

- The MAC address. This is the motherboard Ethernet address on the Voice Gateway Media Card faceplate sticker (for example 00:60:38:01:12:77).
- The ELAN Management IP address of the motherboard Ethernet interface used to perform management through OTM and to communicate with the Meridian 1 and Succession CSE 1000.
- The TLAN Node IP address for the IP Telephony node.
- The TLAN card IP address of the voice interface on each card.
- The IP address of the active ELNK Ethernet interface on the Meridian 1 and Succession CSE 1000 core.

Nortel Networks recommends that you complete an Internet Telephone configuration data summary sheet (Table 46 on page 210) as you install and configure Internet Telephones.

Table 45
Voice Gateway Media Card installation summary sheet

Site________________ Meridian 1 or Succession CSE 1000 system___________________
Meridian 1 and Succession CSE 1000 customer________________________
Node ID (Number)________________________
TLAN Node IP address________________________
Meridian 1 and Succession CSE 1000 active ELNK IP address_______________________
SNMP Manager List IP addresses________________________
TLAN gateway (router) IP address________________________
TLAN subnet mask________________________
ELAN gateway (router) IP address________________________
ELAN subnet mask__________________________

TN	ELAN Management MAC address	ELAN Management IP address	TLAN (Voice) Card IP address	Card role
				Leader
				Follower (OTM: Leader1)
				Follower
				Follower
				Follower
				Follower
				Follower
				Follower
				Follower
				Follower
				Follower
				Follower

Internet Telephone configuration data summary sheet

Table 46
Internet Telephone configuration data summary sheet

No DHCP								
			Partial DHCP					
						Full DHCP		
IP address	subnet mask	Gateway IP address	Connect server IP address*	Node#	VTN	DN	User Name	User Location
*Connect server IP address is the Node IP address of the IP Telephony node.								

Configuration of the DHCP Server

Contents

This section contains information on the following topics:

Reference list

The following are references for this section:

- *Internet Terminals Description* (553-3001-217)

Overview

This chapter provides general guidelines to configure a host with a Dynamic Host Configuration Protocol (DHCP) server to support the i2002 Internet Telephones, i2004 Internet Telephone, and i2050 Software Phone.

> ***Note 1:*** This chapter assumes that you are familiar with RFC 2131 "Dynamic Host Configuration Protocol", RFC 1533 "DHCP Options and BOOTP Vendor Extensions", and the Help manual for the DHCP server on your host. A convenient source for RFCs is http://www.ietf.org/.
>
> ***Note 2:*** For a general overview of DHCP server technology, refer to Appendix E on page 677.
>
> ***Note 3:*** For DHCP server setup and configuration information, refer to Appendix F on page 697.

i2002 and i2004 Internet Telephone, and i2050 Software Phone

The i2002 Internet Telephone, i2004 Internet Telephone, and the i2050 Software Phone are Voice-over Internet Protocol (VoIP) telephones that function as a terminal to the Meridian 1 and Succession Communication Server for Enterprise 1000. The Internet Telephone encodes voice as binary data and packetizes the data for transmission over an IP Network to the Voice Gateway Media Card or to another Internet Telephone.

The Nortel Networks Internet Telephone can act as a DHCP client in one of two modes:

- Partial DHCP mode
- Full DHCP mode

Partial DHCP mode

When the Internet Telephone is configured to operate in partial DHCP mode, the DHCP server needs no special configuration to support Internet Telephones. The Internet Telephone receives the following network configuration parameters from the DHCP server:

- IP address configuration for the Internet Telephone
- Subnet mask for the Internet Telephone IP address
- Default gateway for the Internet Telephone LAN segment

Full DHCP mode

In full DHCP mode, the DHCP server requires special configuration. The Internet Telephone obtains network configuration parameters and connect server configuration parameters from specially configured DHCP servers.

The following configuration parameters are provided for the primary and secondary connect servers:

- Connect server IP address. For IP Line, the connect server IP address is the IP Telephony node IP address.
- A port number of 4100.
- A command value of 1 that identifies the request to the connect server as originating from an Internet Telephone.
- A retry count typically equal to 10.

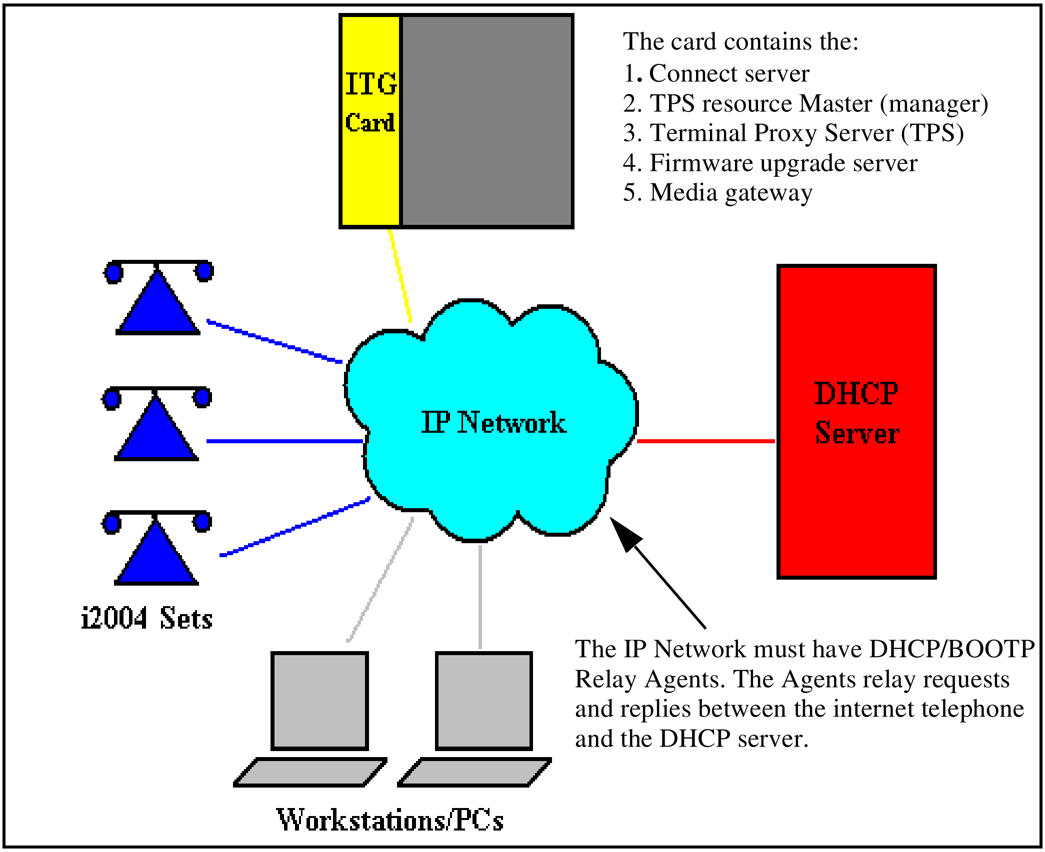
All the configuration parameters for the Internet Telephone can be entered manually. Each Internet Telephone requires the network configuration parameters, connect server parameters, IP Telephony node ID, and Virtual TN. If there are a number of Internet Telephones to configure, manual configuration is time consuming and error prone.

Using Full or Partial DHCP to automatically configure the Internet Telephones is more efficient and flexible. This ensures that current information is used.

Note 1: The IP Telephony node ID and Virtual TN must always be configured manually even in Full DHCP mode.

Note 2: In Partial DHCP mode the connect server parameters, node ID and Virtual TN must be entered manually.

Figure 11
DHCP block diagram



802.1Q Configuration of the i2002/i2004 Internet Telephones

The 802.1Q VLAN support is configured from the user display interface of the i2002/i2004 Internet Telephones. This configuration takes place during the initial configuration procedure of the telephone.

For the 802.1Q configuration procedures of the Internet Telephones, see *Internet Terminals Description* (553-3001-217).

Configuring the DHCP server to support Full DHCP mode

The DHCP capability feature of the Internet Telephone enables the telephone to receive network configuration parameters and specific connect server parameters. This section describes the Internet Telephone's unique class identifier and requested network configuration and connect server parameters for automatic configuration.

Internet Telephone class identifier

The Internet Telephone is designed with a unique class identifier that the DHCP server can use to identify it. All Nortel Networks Internet Telephones use the same text string, "Nortel-i2004-A". The ASCII string is sent inside the Class Identifier option of the Internet Telephone's DHCP messages.

The DHCP server also includes this string in its responses to the Internet Telephone DHCP client. This makes it possible to notify the Internet Telephone that the server is Internet Telephone-aware, and that it is safe to accept the server's offer. This string appears in the beginning of a list of specific Voice Gateway Media Card information that the Internet Telephone DHCP client requests.

When the DHCP server is configured to recognize the Internet Telephone as a special class, the DHCP server can treat the Internet Telephone differently than other DHCP clients. DHCP host configuration parameters can then be grouped by class and only information relevant to the Internet Telephone DHCP client, such as the connect server parameters, is supplied.

Also, the administrator can design the network according to the client's class, if necessary, making maintenance easier. Depending on the capabilities and limitations of the DHCP server used and the design of the network, some of these advanced functions are not available.

Requested Network Configuration Parameters

Nortel Networks Internet Telephones, using Full DHCP mode, can be configured automatically by an Internet Telephone-aware DHCP server by requesting a list of connect server configuration parameters. The Internet Telephone uses DHCP, an industry standard protocol, to request and receive the information.

The Internet Telephones operating in Partial DHCP mode can receive an IP address from any DHCP server. In Full DHCP mode, the server must be configured to respond to the request for the vendor specific encapsulated options.

Table 47 lists the network configuration parameters requested by the Internet Telephone in the Parameter Request List option (Option Code 55) in the DHCPDISCOVER and DHCPREQUEST messages. The DHCPOFFER and the DHCPACK reply messages from the DHCP server must contain the options in Table 47.

Table 47
Internet telephone network configuration requirements (Part 1 of 2)

Parameter Request (Option Code 55)	DHCP Option Code
Subnet mask - the client IP subnet mask.	1
Router/Gateway(s) - the IP address of the client’s default Gateway. (Not required in DHCPOFFER in Internet Telephone Firmware 1.25 and later for compatibility with Novell DHCP server.)	3
Lease Time - implementation varies according to DHCP server.	51

Table 47
Internet telephone network configuration requirements (Part 2 of 2)

Parameter Request (Option Code 55)	DHCP Option Code
Renewal time - implementation varies according to DHCP server.	58
Rebinding interval - implementation varies according to DHCP server.	59
IP Line Site Specific or Vendor Specific encapsulated/site options.	43, 128, 144, 157, 191, 251

The first five parameters in Table 47 are standard DHCP options and have predefined option codes. The last parameter is for Voice Gateway Media Card information, which does not have a standard DHCP option. The server administrator must define a vendor encapsulated and/or site specific option to transport this information to the Internet Telephone.

This non-standard information includes the unique string identifying the Internet Telephone and the connect server parameters for the primary and secondary servers. The Internet Telephone must receive the connect server parameters to connect to the IP Telephony node.

The administrator must use one of the five site specific or vendor encapsulated option codes to implement the Voice Gateway Media Card information. This user-defined option can then be sent as is, or encapsulated in a Vendor Encapsulated option with Option Code 43. The method used depends on the DHCP server's capabilities and what options are already in use by other vendors.

The Internet Telephone rejects any DHCP Offers/Acks that do not contain:

- A Router option. The Internet Telephone requires a default gateway (router).
- A Subnet Mask option.
- Either a Vendor Specific option (see Note 1) or a Site Specific option (see Note 2).

Note 1: The Vendor Specific Option is 43. Windows NT DHCP Server (up to SR4) supports only 16 octets of data for the vendor-specific option, which is insufficient to support the minimum length of the Internet Telephone-specific string. If you use a Windows NT DHCP Server, you must select the Site Specific option to accommodate the Internet Telephone-specific string.

Note 2: The Site Specific options are all DHCP options between 128 (0x80) and 254 (0xFE). These options are reserved for Site Specific use by the DHCP RFCs.

Format for Nortel Networks Internet Telephone DHCP Class Identifier Option

All Nortel Networks Internet Telephones fill in the Class ID option of the DHCP Discovery and Request messages with the null-terminated, ASCII-encoded string Nortel-i2004-A, where A identifies the version number of the information format of the Internet Telephone.

The Class Identifier Nortel-i2004-A must be unique in the DHCP server domain.

Format for Nortel Networks Internet Telephone DHCP Encapsulated Vendor Specific Option

The following definition describes the Nortel specific, Encapsulated Vendor Specific option for the i2002 and i2004 Internet Telephones, and i2050 Software Phone. This option must be encapsulated in a DHCP Vendor Specific Option (refer to RFC 1533) and returned by the DHCP server as part of each DHCPOFFER and DHCPACK message for the Internet Telephone to accept these messages as valid. The Internet Telephone extracts the relevant information from this option and uses it to configure the connect server IP address, the port number (4100), a command value of one, and retry count for the primary and secondary connect servers.

Either this encapsulated vendor specific option or a similarly encoded site specific option must be sent. The DHCP server must be configured to send one or the other but not both. The choice of using either the Vendor Specific or the Site Specific option is provided to enable Windows NT DHCP servers to be used with the Internet Telephone (Windows NT servers do not properly implement the Vendor Specific Option, and as a result, Windows NT implementations must use the Site Specific version).

Format of the option

The format of the Encapsulated Vendor Specific option is Type, Length, and Data as shown below.

Type (1 octet):

There are five choices:

- 0x80 (Site Specific option 128)
- 0x90 (Site Specific option 144)
- 0x9d (Site Specific option 157)
- 0xbf (Site Specific option 191)
- 0xfb (Site Specific option 251)

Providing a choice of five types enables the Internet Telephone to work in environments where the initial choice could already be in use by a different vendor. Pick only one value for TYPE byte.

Length (1 octet)

The Length value is variable. Count only the number of octets in the data field (see below).

Data field (variable number of octets)

The data field contains an ASCII-encoded character string that can be optionally null-terminated. This string can be NULL terminated, although the NULL is not required for parsing.The string is:
"Nortel-i20xx-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr."
where the parameters for the data field are outlined in Table 48 on page 220.

Table 48
Data field parameters

Parameter	Description
Nortel-i2004-A	Uniquely identifies that this is the Nortel option and is a response from a server that can provide the correct configuration information to the i2002 and i2004 Internet Telephones, and the i2005 Software Phone.
ASCII Characters Comma (,) Colon (:) Semicolon (;) Period (.)	ASCII "," separates fields ASCII ":" separates the IP address of the bootstrap server node IP from the Transport Layer port number. ASCII ";" separates the Primary from Secondary bootstrap server information. The bootstrap server is the Active Leader of the IP Telephony node. ASCII "." signals end of structure
iii.jjj.kkk.lll:ppppp	Identifies IP address and port number for server (ASCII encoded decimal)
aaa	Identifies Action for server (ASCII encoded decimal, range 0..255)
rrr	Identifies retry count for server (ASCII encoded decimal, range 0..255)

1. "aaa" and "rrr" are ASCII encoded decimal numbers with a range of 0..255. They identify the "Action Code" and "Retry Count", respectively, for the associated TPS server. They are stored as 1 octet (0x00..0xFF) in the Internet Telephone. These fields must be no more than three digits long.

2. The first server is always considered "Primary"; the second server always considered "Secondary".

3. If only one server is required, terminate primary TPS sequence immediately with "." instead of ";" for example, "Nortel-i20xx-A,iii.jjj.kkk.lll:ppppp,aaa,rrr."

4 Valid options are one or two servers (0 or 3 is not allowed). However, it is recommended that two servers be used. For i2004 Internet Telephone firmware version 3002B00, the valid option is two servers.

Note: If there is only one connect server (that is, only one IP Telephony node is configured), enter the same information for server 1 and server 2.

5 Action code values:

a 0 – reserved

b 1 – UNIStim Hello (currently this type is the only valid choice)

c 2..254 – reserved

d 255 – reserved

6 iii,jjj,kkk,lll are ASCII encoded, decimal numbers representing the IP address of the server. They do not need to be three digits long as the **.** and **:** delimiters guarantee parsing. For example, '001', '01', and '1' would be parsed correctly and interpreted as value 0x01 internal to the Internet Telephone. These fields must be no more than three digits long.

7 ppppp is the port number in ASCII encoded decimal. It does not need to be five digits long as the **:** and **,** delimiters guarantee parsing. For example, '05001', '5001', '1', '00001' would be parsed correctly and accepted as correct. The valid range is 0-65535 (stored internally in the Internet Telephone as hexadecimal in range 0..0xFFFF). This field must be no more than five digits long.

8 In all cases, the ASCII encoded numbers are treated as decimal values and all leading zeros are ignored. Specifically, a leading zero does not change the interpretation of the value to be OCTAL encoded. For example, 0021, 021, and 21 are all parsed and interpreted as decimal 21.

Format for Nortel Networks Internet Telephone DHCP Site Specific Option

The following definition describes the Nortel specific, Site Specific option for the i2002 and i2004 Internet Telephones, and i2050 Software Phone. This option uses the "reserved for site specific use" DHCP options (128 to 254 - refer to RFC 1541 and RFC 1533) and must be returned by the DHCP server as part of each DHCP OFFER and ACK message for the Internet Telephone to accept these messages as valid.

The Internet Telephone retrieves the relevant information and uses it to configure the IP address for the primary and (optionally) secondary TPSs. Either this site specific option must be present or a similarly encoded vendor specific option must be sent (as previously described), that is, configure the DHCP server to send one or the other but not both. The choice of using either Vendor Specific or Site Specific options enables Windows NT DHCP servers to be used with the Internet Telephone. Windows NT servers do not properly implement the Vendor Specific Option and as a result, Windows NT implementations must use the Site Specific version.

Format of the option

The format of the field is Type, Length, Data. The format of the Site Specific Option is the same as the Encapsulated Vendor Specific Option (see “Format of the option” on page 219).

Installation and Initial Configuration of an IP Telephony Node

Contents

This section contains information on the following topics:

Reference list

The following are references for this section:

- *Software Input/Output: Administration* (553-3001-311)
- *Software Input/Output: System Messages* (553-3001-411)
- *Software Input/Output: Maintenance* (553-3001-511)

Overview

This chapter explains how to install and to begin the configuration of new IP Telephony nodes, Voice Gateway Media Cards (ITG-P Line Card and Succession Media Card), and associated cables.

If configuring IP Line 3.0 on a Meridian 1 or Succession Communication Server for Enterprise (CSE) 1000 Rel 1.1 system, the remainder of the configuration of IP Line data must be completed using Optivity Telephony Manager (OTM).

If configuring IP Line 3.0 on a Succession CSE 1000 Release 2.0 system, the remainder of the configuration of IP Line data must be completed using Element Management.

Read the "IP Network Engineering Guidelines" on page 133 before installing an IP Telephony node.

The following is a list of procedures in this chapter:

Equipment considerations

This section lists the required and optional equipment that can be used to install, configure, and maintain the Voice Gateway Media Cards and Internet Telephone products.

Required equipment

The required equipment includes:

- A PC to manage IP Line, with one of the following installed:
  - OTM 2.0 must be installed for Meridian 1 or Succession CSE 1000 Rel 1.1 systems.
  - a Web browser to run Element Management for Succession CSE 1000 Rel 2.0.
- A local TTY or terminal in a switchroom. This is required for Leader configuration.
- Two shielded CAT 5 Ethernet cables to connect the Voice Gateway Media Card to an external switch (recommended) or hub equipment.

- A 10/100BaseT Ethernet port (optional auto-sensing) to support TLAN and 10BaseT ELAN network connections.
- A 10/100BaseT Ethernet port (optional auto-sensing) in each location where an Internet Telephone resides.
- Serial cables.

Optional equipment

The optional equipment includes:

- A server configured with Dynamic Host Configuration Protocol (DHCP). For example, you can use a Nortel NetID server.
- An external modem router to enable remote dial-up connection to ELAN for technical support (The Nortel Networks RM356 modem router is recommended.).

Install the hardware components

There are two cards that use the IP Line 3.0 loadware; the ITG-P Line Card and the Succession Media Card.

- See page 229 for installation instructions for the ITG-P Line Card.
- See page 231 for installation instruction for the Succession Media Card.

  Note: When the IP Line 3.0 loadware is installed on either card, the cards are known as Voice Gateway Media Cards.

Summary of installation steps

The following table summarizes the steps for installing each Voice Gateway Media Card

Table 49
Installation summary (Part 1 of 2)

Step	ITG-P Line Card	Succession Media Card
Determine card slot	See "Identify the IPE card slots" on page 228	See "Identify the IPE card slots" on page 228
Unpack the card	Remove all contents from the packaging box.	Remove all contents from the packaging box.
Install the CompactFlash Card	Not applicable	Procedure 6 on page 232
Install the Voice Gateway Media Cards	Procedure 5 on page 230	Procedure 7 on page 236
Install NTCW84JA ITG-specific I/O Panel Filter Connector for Option 51C/61C/81/81C	Procedure on page 237	Procedure on page 237
Install the NTMF94EA ELAN, TLAN, RS-232 Serial Maintenance I/O interface cable	Procedure 9 on page 243	Not applicable
Install the A0852632 Shielded 50-pin to Serial/ELAN/TLAN Adapter.	Not applicable	Procedure 10 on page 246
Configure card as a Leader or Follower	In OTM: Procedure 24 on page 301 In Element Management: Procedure 43 on page 369 (Leader) Procedure 45 on page 375 (Follower)	In OTM: Procedure 24 on page 301 In Element Management: Procedure 43 on page 369 (Leader) Procedure 45 on page 375 (Follower)

Table 49
Installation summary (Part 2 of 2)

Step	ITG-P Line Card	Succession Media Card
Configure the card properties	In OTM: Procedure 17 on page 282 In Element Management: Procedure 41 on page 362	In OTM: Procedure 17 on page 282 In Element Management: Procedure 41 on page 362
Transmit/Transfer properties	In OTM Procedure 25 on page 303 Procedure 26 on page 305 In Element Management: Procedure 44 on page 372	In OTM Procedure 25 on page 303 Procedure 26 on page 305 In Element Management: Procedure 44 on page 372

Identify the IPE card slots

Depending on the Meridian 1 module you are using, the ITG-P Line Card has to be installed in a certain slot. Use Table 50 to identify the IPE card slots selected for the Voice Gateway Media Card.

Table 50
Voice Gateway Media Card installation by module type

Meridian 1 modules	ITG-P Line Card slots
NT8D37BA/EC IPE modules, NT8D11BC/ED CE/PE modules	All available IPE card slots.
NT8D37AA/DC IPE modules	0, 4, 8, and 12
NT8D11AC/DC CE/PE modules	0

> ***Note:*** EMC restriction must be considered when installing the Voice Gateway Media Cards, for more information see “Electro-magnetic compatibility (EMC)” on page 672.

Installing and cabling the ITG-P Line Card

Each ITG-P Line Card requires two slots in the Meridian 1 and Succession CSE 1000 IPE shelf. Only the left slot of the card connects to the Meridian 1 and Succession CSE 1000 IPE Backplane and I/O panel.

You can install a maximum of eight ITG-P Line Card in an IPE shelf in Option 51C/61C/81/81C. The ITG-P Line Card can occupy any two adjacent slots in an IPE shelf, with the left slot of the card plugging into slots 0 to 6 and 8 to 15. You cannot plug in the left slot of an ITG-P Line Card in slot 7, because the XPEC card is situated in-between slots 7 and 8.

To enable a module to hold the maximum number of ITG-P Line Cards, install each card with the left slot of the card inserted into an even-numbered slot.

CAUTION WITH ESDS DEVICES
Wear an electrostatic discharge strap when handling ITG-P Line Cards. As an additional safety measure, handle all cards by the edges, and when possible, with the loosened packaging material still around the component.

WARNING
The TLAN cable between the ITG-P Line Card and the Layer 2 switch must have a length of 50 meters or less for proper operation of the TLAN interface.

To install an ITG-P Line card, follow the steps in Procedure 5 on page 230.

Procedure 5
Installing the ITG-P Line Card

1 For each ITG-P Line Card in the node, identify the IPE card slot selected for the ITG-P Line Card. Use the information from the “Voice Gateway Media Card installation summary sheet” on page 208, and Table 45 on page 209.

Table 51
ITG-P Line Card installation by module type

Meridian 1 Modules	ITG-P Line Card
NT8D37BA/EC IPE modules, NT8D11BC/ED CE/PE modules	All available IPE card slots.
NT8D37AA/DC IPE modules	0, 4, 8, and 12
NT8D11AC/DC CE/PE modules	0

Note: Even though the ITG-P Line Card is a two-slot card, only the left slot is counted for the card slot number. For example, for an ITG-P Line Card installed in slots 2 and 3, the slot number is 2.

2 Remove any existing I/O panel cabling associated with any card previously installed in the selected card slot.

3 Insert the ITG-P Line Card into the card guides and gently push it until it makes contact with the backplane connector. Hook the locking devices.

Note 1: The red LED on the faceplate remains lit until the card is configured and enabled in the loadware, at which point it turns off.

Note 2: The faceplate display window displays startup self-test results (T:xx) and status messages. A display “F:XX” indicates a failure of the self-test. It is normal for the ITG-P Line Card to display “F:10” during the start-up self-test. F:10 indicates that the self-test did not find a Security Device. The ITG-P Line Card does not have a security device. Some failures indicate that the card must be replaced. See Table 69 on page 553 for a list of the ITG-P Line Card display codes.

End of Procedure

Installing and cabling the Succession Media Cards

The Succession Media Card is the successor of the ITG-P Line card. It increases the packet processing power of the ITG-P Line card, increases the channel density from 24 to 32 ports, and reduces the slot count from a dual slot to a single IPE slot.

The Succession Media card requires only one slot in the Meridian 1 and Succession CSE 1000 IPE shelf.

CAUTION WITH ESDS DEVICES
Wear an electrostatic discharge strap when handling Succession Media Cards. As an additional safety measure, handle all cards by the edges, and when possible, with the loosened packaging material still around the component.

CompactFlash installation

The Succession Media Card package contains the following items:

- Succession Media Card
- CompactFlash card
- Retaining Pin

The CompactFlash must be installed on the Succession Media Card prior to installing the card in the system. Follow the steps in Procedure 6 on page 232 to install the CompactFlash.

> ***Note:*** If it is necessary to remove the CompactFlash card, follow the steps outlined in Procedure 92 on page 595.

Procedure 6
Installing the CompactFlash on the Succession Media Card

1 Remove the Succession Media Card, CompactFlash, and Retaining Pin from the packaging.

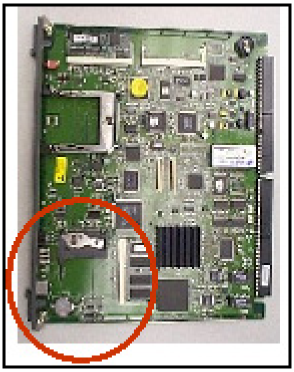
CAUTION WITH ESDS DEVICES
Observe the necessary precautions for handling ESD sensitive devices. Wear a properly connected anti-static wrist strap while removing the cards from the packaging and work on a static dissipative surface.

The CompactFlash and Retaining Pin are shown in Figure 12 on page 232.

Figure 12
CompactFlash Card and Retaining Pin

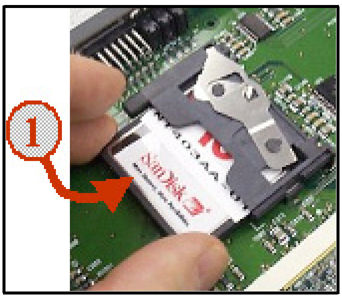
2 Locate the CompactFlash socket in the lower left-hand corner of the Succession Media card (see Figure 13 on page 233).

Figure 13
CompactFlash socket on Succession Media Card



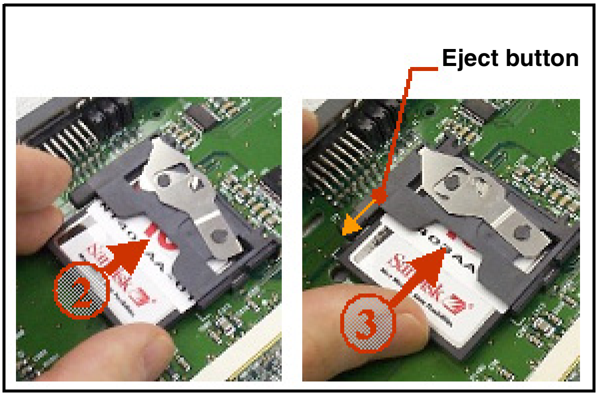
3 Position the CompactFlash card with the label facing up and contact pins toward the socket as shown in Figure 14 on page 233.

Figure 14
Position the CompactFlash in socket



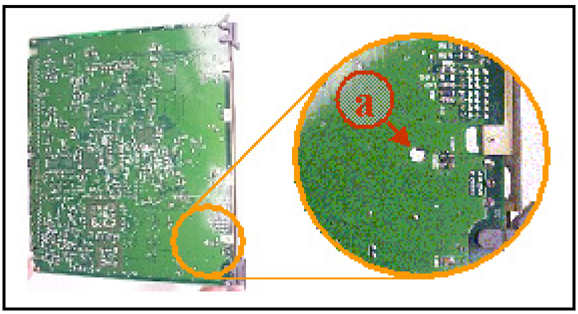
4 Insert the CompactFlash card in the socket. Press firmly until it is fully seated and the Eject button extends (see Figure 15 on page 234).

Figure 15
Insert CompactFlash to extend Eject button



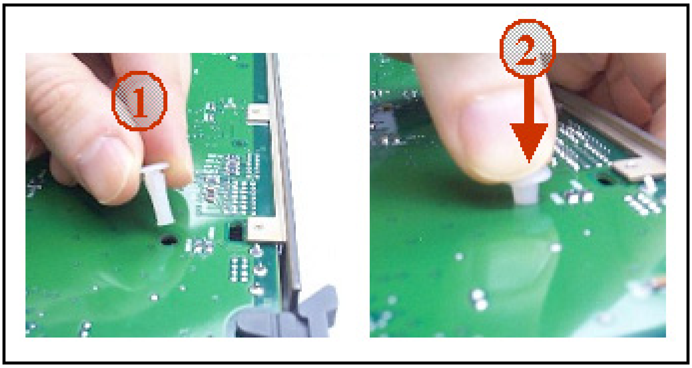
5 Turn the Succession Media Card over to view the back of the card. Identify the hole for the Retaining Pin. The hole (labeled ***a*** in Figure 16) is located approximately 1 inch (2.5 cm) above the lower lock latch and 1 inch (2.5 cm) from the card's faceplate.

Figure 16
Retaining Pin hole



6 Insert the Retaining Pin in this hole (labeled **1** in Figure 17). Press the Retaining Pin into the hole until the pin clicks as it locks into position (labeled **2** in Figure 17). The underside of the head of the Retaining Pin should be flat against the card.

Figure 17
Inserting the Retaining Pin



7 Turn the card over to view the front of the card. Ensure the Retaining Pin is in place as shown Figure 18.

Figure 18
Retaining Pin fully inserted

End of Procedure

To install an Succession Media Card, follow the steps in Procedure 7 on page 236.

Procedure 7
Installing the Succession Media Card

1 For each Succession Media Card in the node, identify the IPE card slot selected for the Succession Media Card. Use the information from the "Voice Gateway Media Card installation summary sheet" on page 208, and Table 45 on page 209.

Table 52
Succession Media Card installation by module type

Meridian 1 Modules	Succession Media Card
NT8D37BA/EC IPE modules, NT8D11BC/ED CE/PE modules	All available IPE card slots.
NT8D37AA/DC IPE modules	0, 4, 8, and 12
NT8D11AC/DC CE/PE modules	0

2 Remove any existing I/O panel cabling associated with any card previously installed in the selected card slot.

3 Insert the Succession Media Card into the card guides and gently push it until it makes contact with the backplane connector. Hook the locking devices.

Note 1: The red LED on the faceplate remains lit until the card is configured and enabled in the loadware, at which point it turns off.

Note 2: The faceplate display window displays startup self-test results (T:xx) and status messages. A display "F:xx" indicates a failure of the self-test. Some failures indicate that the card must be replaced.

Note 3: Refer to "Transfer IP Telephony node configuration from Element Management to the Voice Gateway Media Cards" on page 368.

Note 4: Refer to Table 70 on page 555 for a listing of the Succession Media Card display codes.

End of Procedure

Installing the NTCW84JA ITG-specific I/O Panel Filter Connector for the Option 51C/61C/81/81C

For Meridian 1 Option 51C/61C/81/81C, the standard IPE module I/O filtering is provided by the 50-Pin filter connectors mounted in the I/O Panel on the back of the IPE shelf. The filter connector attaches externally to the MDF cables and internally to the NT8D81AA Backplane to the I/O Panel ribbon cable assembly.

For 100BaseTX TLAN operation, the standard I/O filter connector must be replaced with the NTCW84JA ITG Line-specific I/O filter connector for:

- the leftmost of the two card slots occupied by the NTVQ55AA ITG-P Line Card
- the slot occupied by the NTVQ01BA Succession Media Card

For Option 11C, 11C-Mini, and Succession CSE 1000 systems, the standard I/O filter connector already supports 100BaseTX TLAN operation.

To replace an existing I/O Panel Filter Connector, follow the steps in Procedure 8 on page 238.

> ***Note:*** This NTCW84JA ITG-specific Filter Connector is not required on Option 11C, 11C-Mini, or Succession CSE 1000 systems.

CAUTION

For Option 51C/61C/81/81C manufactured between 1998-1999 and shipped in North America, the IPE modules have the NT8D81BA Backplane to I/O Panel ribbon cable assembly with a non-removable Filter Connector. The NT8D81BA is compatible with 10BaseT TLAN, but if you require a 100BaseT TLAN, you must order the NT8D81AA Backplane to I/O Panel ribbon cable assembly to replace it. Do not install the NTCW84JA ITG-specific Filter Connector onto the existing non-removable Filter Connector.

Replace existing I/O panel Filter Connector

The standard I/O Filter Connector is shielded metal with a black plastic insert connector. The NTCW84JA connector uses yellow warning labels to indicate EMC filtering modifications and which MDF connection points can support 100BaseT connections.

Procedure 8
Replacing the existing I/O Panel Filter Connector

1 Before any of the following steps, remove the ITG pack, or any other IPE pack, from the IPE shelf card slot corresponding to the I/O Panel connector to be removed.

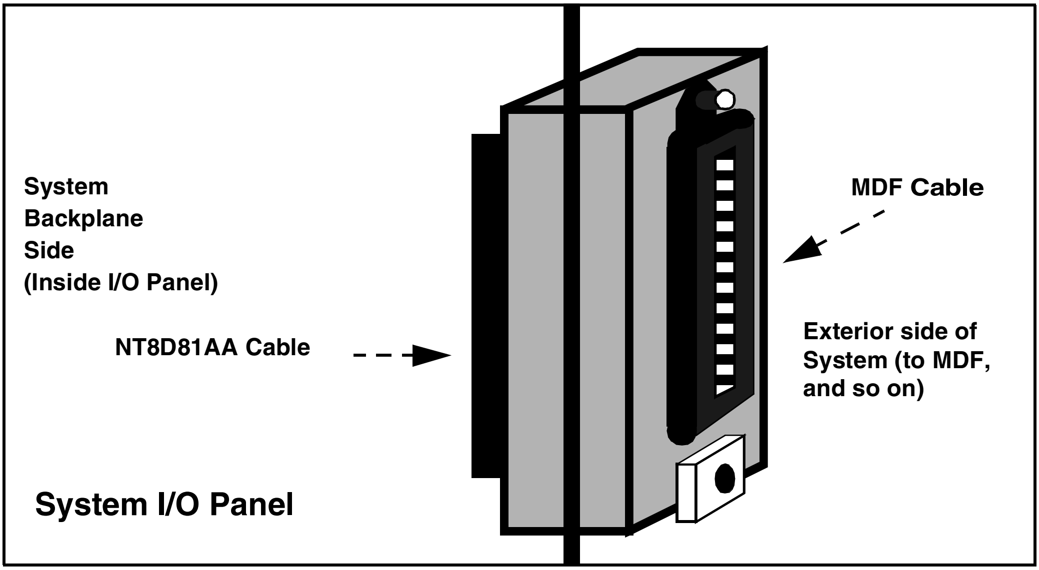
Note: Make sure to use the I/O Panel Filter Connector which corresponds to the left slot number of the DCHIP card.

2 Remove the NT8D81AA Backplane to I/O Panel ribbon cable assembly, that is connected to the Backplane side of the existing block, by releasing the latching pins on the filter block and pulling the NT8D81AA cable away.

3 Unscrew the existing Filter Connector from the I/O panel. There is one screw on the lower front of the connector and one screw on the upper back of the connector. Remove the connector.

4 Re-position the new NTCW84JA Filter Connector in the now vacant I/O panel opening (see Figure 19 on page 239).

Figure 19
NTCW84JA 50 pin ITG-specific I/O Panel Filter Connector for Option 51C/61C/81/81C



5 Attach the new NTCW84JA ITG-specific Filter Connector to the I/O panel by securely fastening the top back screw and the bottom front screw.

6 Reconnect the NT8D81AA cable and secure it in place by snapping shut the locking latches provided on the NTCW84JA connector.

End of Procedure

Incorrect configuration problems

TLAN operation problems can arise from the standard I/O filter connector in IPE modules on Meridian 1 System Option 51C/61C/81/81C. Some problems scenarios and their respective solutions are outlined in Table 53:

Table 53
I/O filter connector

Scenario	Solution
The installer forgets to replace the standard IPE module I/O filter connector with the provided Voice Gateway Media Card/ITG-specific filter connector that removes filtering from pairs 23 and 24.	Correctly install the Voice Gateway Media Card/ITG-specific filter connector by replacing the standard IPE Module I/O filter connector.
The installer installs the Voice Gateway Media Card/ITG-specific filter connector on top of the standard IPE module I/O filter connector.	Correctly install the Voice Gateway Media Card/ITG-specific filter connector by replacing the standard IPE Module I/O filter connector.
The installer encounters an IPE module that is equipped with standard filter connectors molded onto the backplane I/O ribbon cable assemblies. The installer does not replace the IPE module backplane I/O ribbon cable assemblies with the ones that have interchangeable I/O filter connectors.	Order new IPE Module Backplane I/O ribbon cable assemblies that have interchangeable I/O filter connectors if it becomes necessary to use one of the IPE Modules with molded-on I/O filter connectors.
The TLAN UTP cabling does not meet the UTP Cat. 5 termination and impedance uniformity standards.	Always ensure that TLAN UTP cabling as installed is Cat. 5 compliant.

Voice Gateway Media Card ELAN and TLAN Interfaces

The ELAN and TLAN interfaces are provided by one of the following:

- NTMF94EA ELAN, TLAN, RS-232 Serial Maintenance I/O interface cable (see Figure 20 on page 242)
- A0852632 Shielded 50-pin to Serial/ELAN/TLAN Adapter (see Figure 21 on page 244)

The ITG-P Line Card uses the NTMF94EA ELAN, TLAN, RS-232 Serial Maintenance I/O interface cable.

The Succession Media Card uses A0852632 Shielded 50-pin to Serial/ELAN/TLAN Adapter.

The ELAN supports 10BaseT operation and the TLAN supports 10/100BaseT operation. To support the 100BaseT operation on Meridian 1 Option 51C/61C/81/81C the TLAN interface requires specialized I/O panel mounting connectors. These replace the standard connectors provided on the Meridian 1 system.

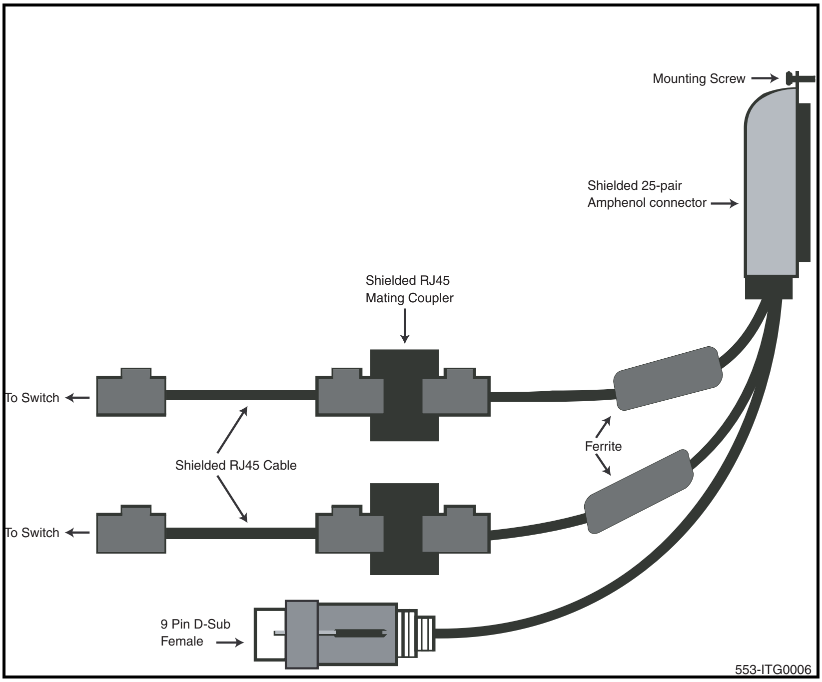
Cables and connectors for the ELAN and TLAN interface functions include:

- the NTCW84JA Meridian 1 Option 51C/61C/81/81C I/O panel filter block
- NTMF94EA ELAN, TLAN, RS-232 Serial Maintenance I/O interface cable
- A0852632 Shielded 50-pin to Serial/ELAN/TLAN Adapter. Standard shielded, CAT-5 LAN cables (<100 meters) are recommended to attach the LAN ports to the local network.

Install the NTMF94EA ELAN, TLAN, RS-232 Serial Maintenance I/O interface cable

The NTMF94EA cable provides the ELAN, TLAN and serial interface for the NTVQ5AA ITG-P Line Card. See Appendix : "NTMF94EA I/O cable" on page 634 for pinouts and technical specifications on the NTMF94EA cable.

Figure 20
NTMF94EA ELAN, TLAN, and RS-232 Serial Maintenance I/O cable



To install the NTMF94EA ELAN, TLAN, serial interface cable, complete the steps in Procedure 9.

Procedure 9
Installing the NTMF94EA ELAN, TLAN, serial interface cable

> **WARNING**
> Plug all Voice Gateway Media Cards ELAN interfaces belonging to the same node into the same ELAN hub or Layer 2 switch port group.

1 On Option 51C/61C/81/81C, connect the NTMF94EA ELAN, TLAN, and RS232 Serial Maintenance I/O cable to the I/O panel connector for the left hand card slot.

If you have an Option 11C or 11C-Mini, connect the cable to the I/O connector in the cabinet that corresponds to the IP Line card slot (see Figure 167 on page 635).

2 Connect a shielded Category 5 cable from the customer's TLAN switch equipment to the port labeled "T-LAN".

3 Connect a shielded Category 5 cable from the customer's ELAN hub or switch equipment to the port labeled "E-LAN".

4 Install the NTAG81CA serial cable into the faceplate Maintenance port. This connection is used to configure the IP address for Leader 0. If required, use the NTAG81BA maintenance extender cable.

Note: Alternatively, for a permanent connection to the maintenance port, use the DB9 female connector on the NTMF94BA breakout cable to connect a modem (using a null modem) or directly to a local TTY terminal.

> **WARNING**
> The serial maintenance ports presented at the faceplate and at the backplane are identical. Do not connect a terminal to both access points simultaneously. This results in incorrect and unpredictable operation of the Voice Gateway Media Card.

Note 1: The switch LEDs and the faceplate link LEDs light when you connect the card to the WAN/LAN through the TLAN port.

Note 2: Refer to “IP Network Engineering Guidelines” on page 133 for more details about engineering and connecting the LAN/WAN.

End of Procedure

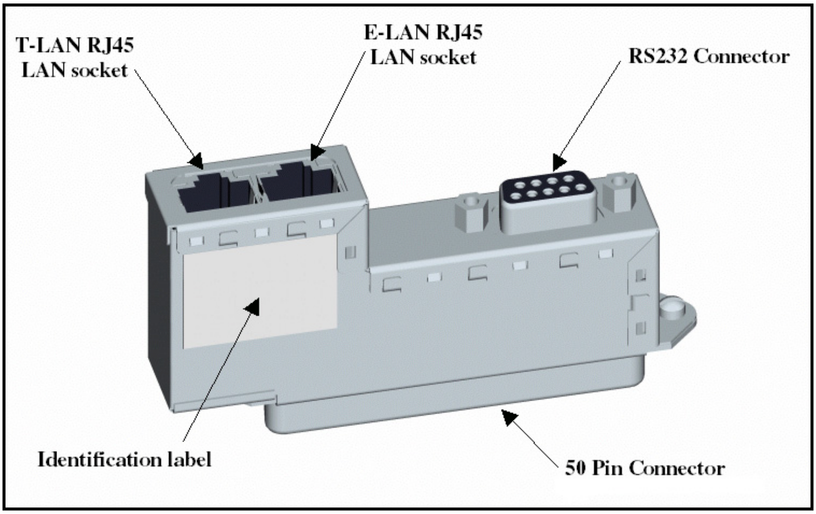
Install the Shielded 50-pin to Serial/ELAN/TLAN Adapter

The Succession Media Card can support a single connector solution for access to the TLAN and ELAN Ethernet Ports. This connector (see Figure 21 on page 244) is called the A0852632 Shielded 50-pin to Serial/ELAN/TLAN Adapter solution and it replaces a single NTMF94EA ELAN, TLAN, RS-232 Serial Maintenance I/O interface cable (‘octopus’ cable).

The adapter breaks out the signals from the I/O connector to the following:

- Ethernet management port (ELAN)
- telephony port (TLAN)
- one RS232 (local console) port

Figure 21
Shielded 50-pin to Serial/ELAN/TLAN Adapter



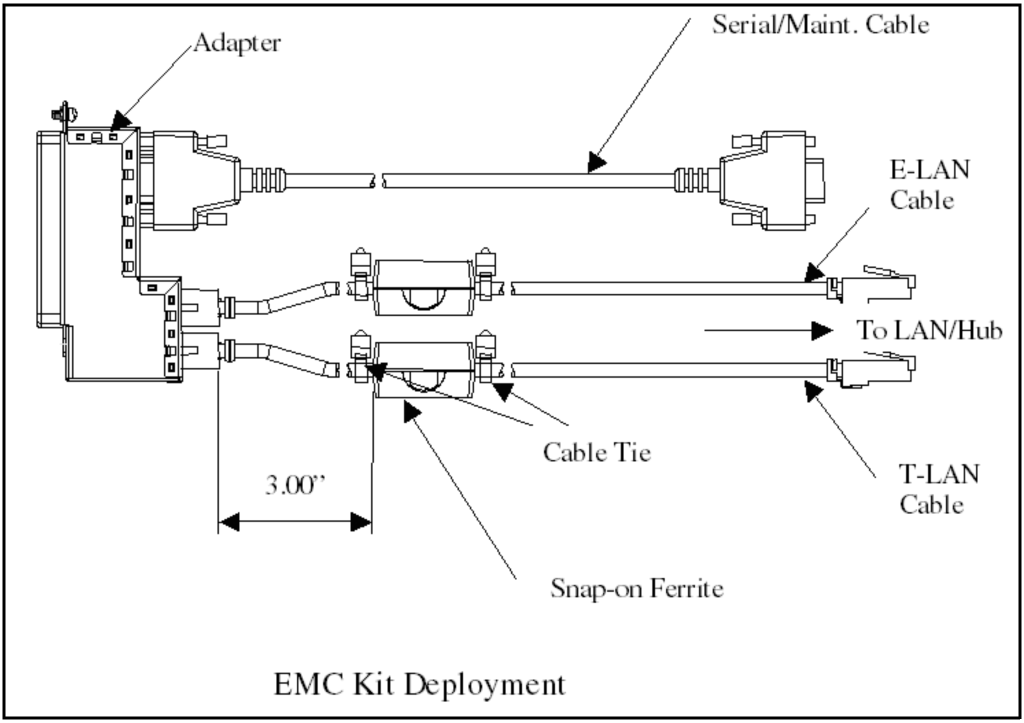
On Option 51C/61C/81/81C, the NT8D81AA cable is used to bring all 24 Tip and Ring pairs to the I/O panel. The NTCW84JA I/O panel mounting block must be installed on large systems before the A0852632 Shielded 50-pin to Serial/ELAN/TLAN Adapter is installed. Refer to Figure 21 on page 244.

To ensure proper connection, install the adapter securely; otherwise, connectivity could be lost.

EMC Shielding Kit

An ITG EMC shielding kit (NTVQ83AA) must be installed on the ELAN and TLAN interface cables to meet regulatory requirements at the installation site. As shown in Figure 22 on page 246, a ferrite must be placed on both the ELAN and TLAN Ethernet cables during installation. Cable ties are then placed to retain the ferrites in the correct position. This applies to Option 11C/11C-Mini and Option 51C/61C/81/81C.

Figure 22
ITG EMC Shielding Kit Deployment



Procedure 10
Installing the Shielded 50-pin to Serial/ELAN/TLAN Adapter onto the Succession Media Card

1 Install the Shielded 50-pin to Serial/ELAN/TLAN Adapter into the card connector (1, 2, 3, or 4) where the Succession Media Card is located.

2 Connect a shielded Category 5 cable from the customer's TLAN switch equipment to the port labeled "T-LAN".

3 Connect a shielded Category 5 cable from the customer's ELAN hub or switch equipment to the port labeled "E-LAN".

4 Install the NTAG81CA serial cable into the faceplate Maintenance port.

End of Procedure

Initial configuration of IP Line data on Meridian 1 and Succession Communication Server for Enterprise 1000

Summary of Procedures

1. Configure IP address for the Meridian 1 and Succession CSE 1000 ELNK Ethernet Interface (LD 117) (see page 248).
2. Configure VoIP bandwidth management zones (LD 117) (see page 249).
3. Configure physical TNs (LD 14) (see page 253).
4. Configure virtual superloops for Internet Telephones (LD 97) (page 259).
5. Configure Internet Telephone features (LD 11) (see page 263).

Before you begin

- Verify the software release running on your system.
  - The minimum required software release to support all the features of IP Line 3.0 is Succession CSE 1000 Release 2.0.
  - IP Line 3.0 runs on Meridian 1 and Succession CSE 1000 Release 1.0/1.1; however, not all the IP Line 3.0 features are available.
- Verify the ISM System Limit in LD 22. The ISM system limit must have sufficient unused units to support the number of Internet Telephones you are installing. Refer to the *Software Input/Output: Maintenance* (553-3001-511).
- Expand the ISM System Limit, if required, by ordering additional ISM Parameters. See Table 4 on page 28, and “ISM parameters” on page 127.

Configure IP address for the Meridian 1 and Succession CSE 1000 ELNK Ethernet Interface (LD 117)

To configure the ELAN IP address for the Meridian 1 and Succession CSE 1000 active ELNK Ethernet interface, follow the steps in Procedure 11.

Procedure 11
Configuring the ELAN IP address for the Meridian 1 and Succession CSE 1000 active ELNK Ethernet interface

1 Go to LD 117.

2 Create host entries with IP address on the ELAN subnet by entering one of the following commands:

NEW HOST PRIMARY_IP xx.xx.xx.xx

NEW HOST SECONDARY_IP xx.xx.xx.xx (for Option 61C and Option 81/81C only)

3 Assign host entry IP address to active and inactive ELNK interfaces on ELAN by entering one of the following commands:

CHG ELNK ACTIVE PRIMARY_IP

CHG ELNK INACTIVE SECONDARY_IP (for Dual CPU only)

4 Verify the IP address for the Ethernet by entering the following command: **PRT ELNK**.

5 Enter the following: **Update DBS**.

6 Go to LD 137. Check the status of the Ethernet interface by entering the command: **STAT ENLK**. If the ELNK is disabled, enable it by entering: **ENL ELNK**.

End of Procedure

Configure VoIP bandwidth management zones (LD 117)

Up to 256 zones can be defined in LD 117. The Call Server uses the zones for VoIP bandwidth management. For more information, see “VoIP bandwidth management zones” on page 164.

The term Intrazone means within the same zone, and Interzone means between two different zones.

Table 54 on page 250 lists the four zone parameters as:

- p1 - Total bandwidth (Kbps) available for Intrazone calls.
- p2 - Defines the codec for Intrazone calls (that is, preserve voice quality or preserve bandwidth). BQ provides Best Quality but uses the most bandwidth, whereas BB uses the least amount of Bandwidth but reduces voice quality.
- p3 - The total bandwidth available for Interzone calls.
- p4 - The preferred strategy for the choice of the codec for Interzone calls
- p5 - The zone resource type. The type is either shared or private.

LD 117 also includes DIS and ENL commands to disable or enable a zone. When a zone is created, its default state is enabled.

> **CAUTION**
> Zone 0 must be configured in LD 117 before other zones are configured or all calls associated with zone 0 are blocked.

Table 54
LD 117 bandwidth management zones configuration

Command	Description
NEW ZONE xxx p1 p2 p3 p4 p5	User creates a new zone, where: xxx = zone number = (0) - 255. p1 = Intrazone available bandwidth = 0 - (10000) - 100000 (Kbps) p2 = Intrazone preferred strategy = (BQ for Best Quality) or BB for Best Bandwidth p3 = Interzone available bandwidth = 0 - (10000) - 100000 (Kbps) p4 = Interzone preferred strategy = BQ for Best Quality or BB for Best Bandwidth p5 = Zone resource type = (shared) or private
New ZONE xxx	User creates a new zone with default values for the parameters: p1 = 10000 (Kbps) p2 = BQ p3 = 10000 (Kbps) p4 = BQ p5 = shared
CHG ZONE xxx p1 p2 p3 p4 p5	User changes parameters of a zone. All parameters must be re-entered, even those that are unchanged.
OUT ZONE xxx	User removes a zone.
DIS ZONE xxx	Allows user to disable a zone. When a zone is disabled, no new calls are established inside, from, or toward this zone.
ENL ZONE xxx	Allows user to enable a zone.
PRT ZONE xxx	Prints zone and bandwidth information.

Element Management GUI for Zone Configuration

In the Succession CSE 1000 Rel 2.0 system, the user can optionally configure zones using Element Management instead of using LD 117.

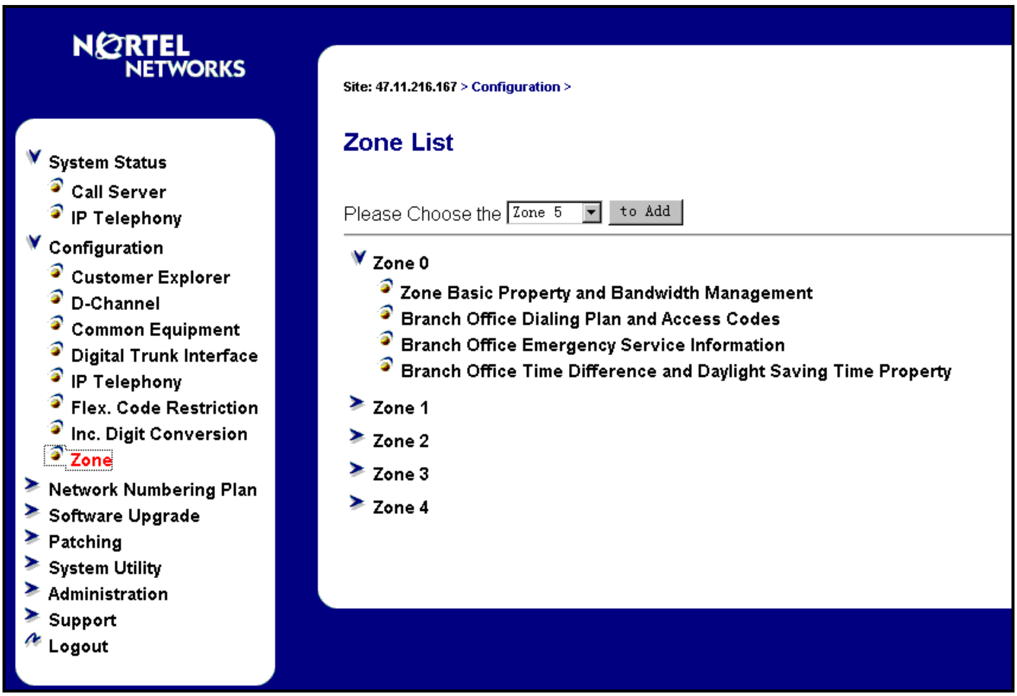
To view Element Management GUI for zone configuration, perform the steps in Procedure 13 on page 256:

Procedure 12
Viewing Element Management GUIs for Zone Configuration

1 Launch and log in to Element Management. See Procedure 33 on page 335.

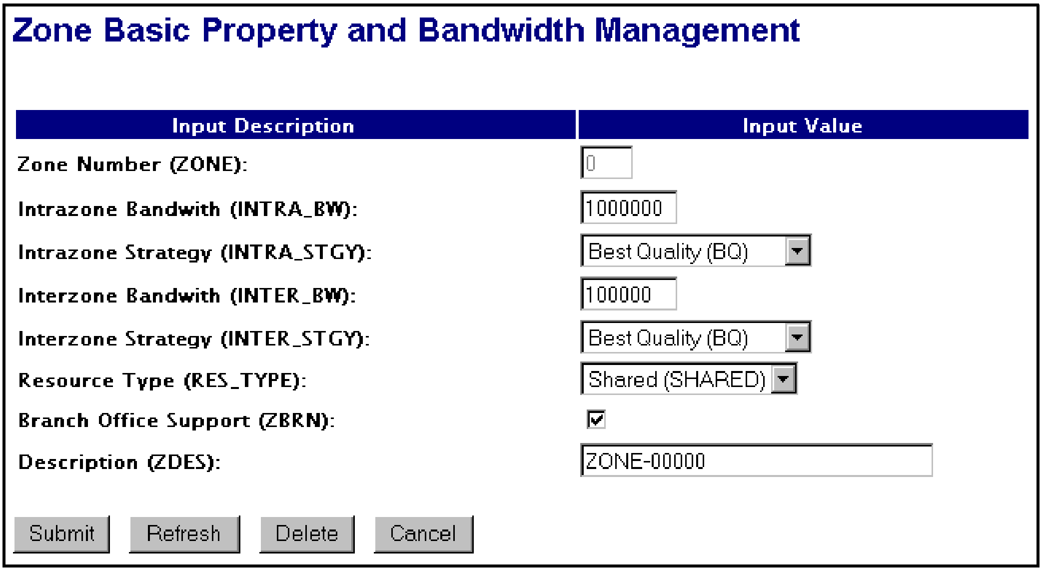
2 In the Navigation Tree, click **Configuration** and then click **Zones**. The **Zones List** appears.

Figure 23
Zone List



3 Click the **to Add** button to add a new zone. The **Zones Basic Property and Bandwidth Management** pages.

Figure 24
Zones Basic Property and Bandwidth Management



End of Procedure

Configure physical TNs (LD 14)

Use LD 14 to define the physical TNs for the Voice Gateway Media Card.

ITG Line 2.2 introduced a new LD 14 prompt **IPTN** (ITG Physical TN) to differentiate the Voice Gateway Media Card voice media gateway channels from the IP trunk units of an ITG trunk 2.0 card.

There are three new responses that have been added with the addition of the Succession Media Card. Both changes are in LD 14. The three new responses are:

- REQ: **New 32**—the Succession Media Card has 32 voice media gateway channels
- XTRK **ITG1**—since Succession Media Card is a one slot card this enables the next slot to be configured.
- MAXU **32**—instead of a maximum of 24 gateway channels on the ITG-P Line Card, there are 32 gateway channels with the Succession Media Card.

Use LD 14 to disable the newly-created IPTN cards. The OTM IP Telephony Gateway - IP Line 3.0 application requires Voice Gateway Media Cards to be in a disabled state before transmitting card properties.

See Table 55 for a list of the prompts and responses in LD 14.

Table 55
Configure physical TNs in LD 14 (Part 1 of 2)

Prompt	Response	Description
REQ:	NEW 24 NEW 32	Create 24 voice media gateway channels on an ITG-P Line Card. Create 32 voice media gateway channels on a Succession Media Card.
TYPE:	TIE	TIE Trunk. There is no route datablock required for IPTNs.
TN	l s c u c u	TN of the first ITG Physical TN (Option 51C/61C/81/81C) (Option 11C TN format).

Table 55
Configure physical TNs in LD 14 (Part 2 of 2)

Prompt	Response	Description
DES	aa.......a	Description for gateway channel. Identify the channel using the card's TLAN IP address or MAC address.
XTRK	itg1 itg2	ITG1 is the Succession Media Card which occupies only 1 card slot. ITG1 enables the next card to be configured in the next slot. ITG2 is the NTVQ55AA ITG-P Line card which occupies 2 card slots. ITG2 instructs the software to skip the next slot when configuring trunk units. (Slot cannot be used because this is a dual slot card.) ***Note:*** Entering ITG2 at the XTRK prompt works for the Succession Media Card; however, the next slot cannot be configured or used.
MAXU	32 24	32 is the maximum number of voice media gateway channels on the Succession Media Card. 24 is the maximum number of voice media gateway channels on the ITG-P Line Card.
IPTN	YES	ITG Physical TN.
ZONE	0 - 255	Zone number to which this ITG Physical TN belongs. Verify that the zone exists in LD 117.
CUST	0 - 99	The customer to which the IPTN resources are assigned. ***Note:*** This means that for multi-customer Meridian 1 and Succession CSE 1000 systems, each customer must have a dedicated IP Telephony node for Internet Telephones.

See Table 56 for a list of LD 14 OUT command.

Table 56
LD 14 OUT command

Prompt	Response	Description
REQ:	OUT 24	Delete 24 voice media gateway channels on an ITG-P Line Card.
	OUT 32	Delete 32 voice media gateway channels on a Succession Media Card.
	OUT 32	Delete 8 voice media gateway channels on a Succession Media Card.
TYPE:	TIE	TIE Trunk.
TN	l s c u c u	TN of the first ITG Physical TN (Option 51C/61C/81/81C) (Option 11C TN format).

See Table 57 for a list of LD 14 CHG command.

Table 57
LD 14’s CHG command

Prompt	Response	Description
REQ:	CHG	Change configuration data for a gateway channel.
TYPE:	TIE	TIE Trunk.
TN	l s c u c u	TN of the first ITG Physical TN (Option 51C/61C/81/81C) (Option 11C TN format).
DES	aa.......a	Description for gateway channel. Identify the channel using the card’s TLAN IP address or MAC address.
ZONE	0 - 255	Zone number to which this ITG Physical TN belongs. Verify that the zone exists in LD 117.

Element Management GUI for Gateway Channels

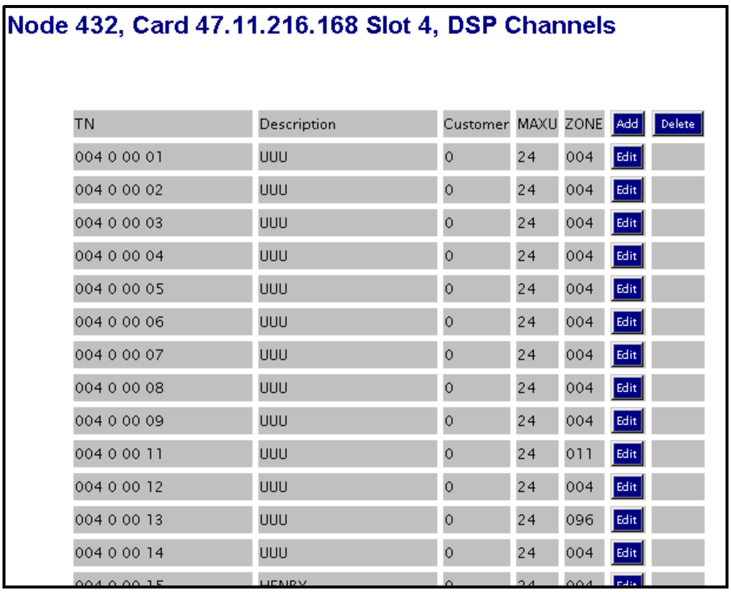
In the Succession CSE 1000 Rel 2.0 system, the user can optionally configure the Gateway Channels using Element Management instead of using LD 14.

To view Element Management GUI for Gateway Channels, perform the steps in Procedure 13 on page 256.

Procedure 13
Viewing Element Management GUIs for Gateway Channels

1. Launch and log in to Element Management. See Procedure 33 on page 335 for details.
2. In the Navigation Tree, click **Configuration** and then click **IP Telephony**. The Node Summary Page appears.
3. Expand a node by clicking the arrow to the left of the node. Click the **DSP Channels** button. The Gateway Channel summary page opens (see Figure 25 on page 256).

Figure 25
Gateway Channel summary page

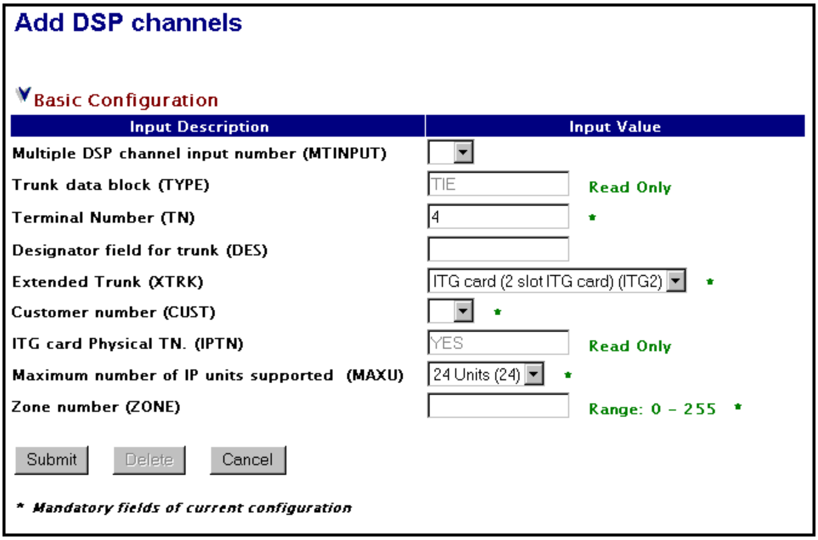

Node 432, Card 47.11.216.168 Slot 4, DSP Channels

TN	Description	Customer	MAXU	ZONE	Add	Delete
004 0 00 01	UUU	0	24	004	Edit	
004 0 00 02	UUU	0	24	004	Edit	
004 0 00 03	UUU	0	24	004	Edit	
004 0 00 04	UUU	0	24	004	Edit	
004 0 00 05	UUU	0	24	004	Edit	
004 0 00 06	UUU	0	24	004	Edit	
004 0 00 07	UUU	0	24	004	Edit	
004 0 00 08	UUU	0	24	004	Edit	
004 0 00 09	UUU	0	24	004	Edit	
004 0 00 11	UUU	0	24	011	Edit	
004 0 00 12	UUU	0	24	004	Edit	
004 0 00 13	UUU	0	24	096	Edit	
004 0 00 14	UUU	0	24	004	Edit	
004 0 00 15	HENRY	0	24	004	Edit	

4 To add new gateway channels, click the **Add** button in the Gateway Channel summary page.

Figure 26 on page 257 shows the GUI equivalent to LD 14's NEW command.

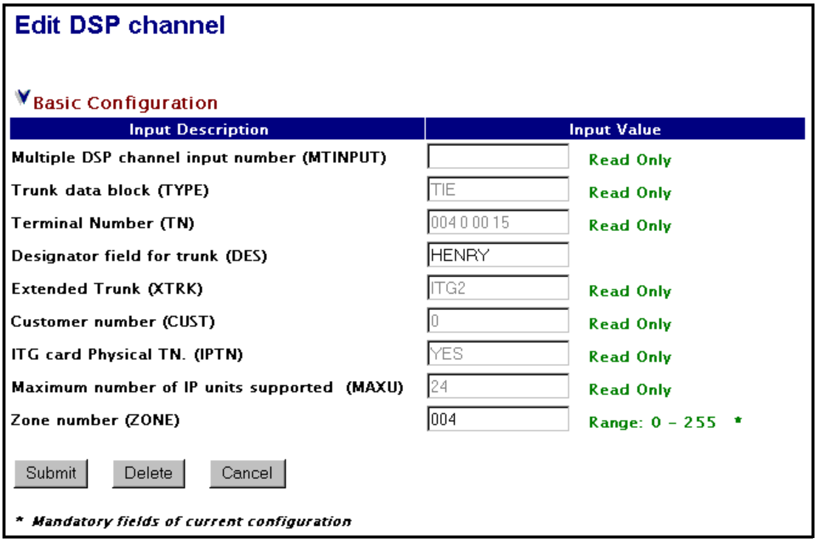
Figure 26
Add gateway channel



5 To edit a particular gateway channel, click the Edit button to the right of the channel on the Gateway Channel summary page.

Figure 27 on page 258 shows the gateway channel's Edit page. This figure is the GUI equivalent to LD 14's CHG command that enables the changing of the DES and ZONE parameters of the channel.

Figure 27
Edit gateway channel

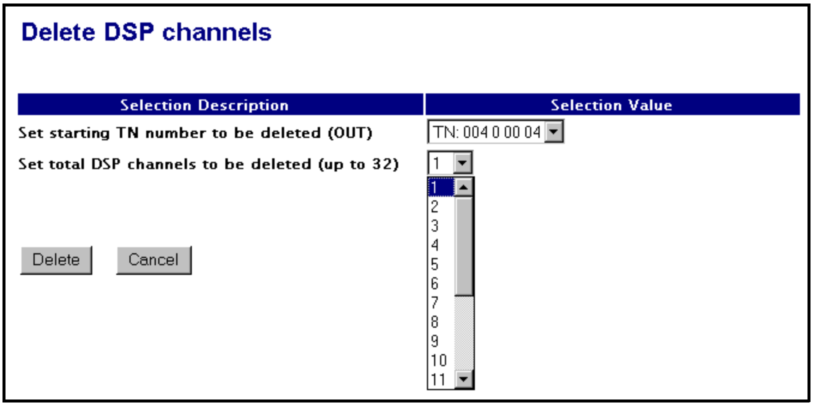


6 To delete a gateway channel, click the **Delete** button in the Gateway Channel summary page (see Figure 25 on page 256).

The Delete page for the gateway channel opens (see Figure 28 on page 259). Select a gateway channel from the drop-down list box and click **Delete**.

Figure 28 shows the GUI equivalent to LD 14’s OUT command.

Figure 28
Delete gateway channel



End of Procedure

Configure virtual superloops for Internet Telephones (LD 97)

One or more virtual superloops must be configured to support Internet Telephone Virtual TNs (VTNs).

Option 51C/61C/81/81C

In Option 51C/61C/81/81C, virtual superloops contend for the same range of loops with phantom, standard and remote superloops, digital trunk loops and all service loops. Virtual superloops can reside in physically equipped network groups or in virtual network groups.

Without FIBN, Package 365, there is a maximum of five network groups available, 0 - 4. With Package 365, there are a maximum of eight network groups, 0 - 7. For normal traffic engineering, provision up to 1024 VTNs on a single virtual superloop for an Option 51C/61C/81/81C. For non-blocking, do not exceed 120 VTNs on a single virtual superloop, for an Option 51C/61C/81/81C.

Nortel Networks recommends that Virtual Superloops are configured starting in the highest non-physically equipped group available. Table 55 lists the prompts and responses required to configure virtual superloops in LD 97.

Table 58
Virtual Superloop configuration in LD 97

Prompt	Response	Description
REQ:	CHG	Change.
TYPE:	SUPL	Superloop.
SUPL	Vxxx	V stands for a virtual superloop and xxx is the number of the virtual superloop. xxx = 0-156 and multiple of four for Option 51C/61C/81/81C without FIBN package 365. xxx = 0-252 and multiple of four for Option 51C/61C/81/81C with FIBN package 365. xxx = 96-112 and multiple of four for Option 11C and 11C-Mini.

Option 11C/11C-Mini

In Option 11C/11C-Mini, virtual superloops contend for the same range of superloops, 96-112, with phantom superloops.

Up to 128 VTNs can be configured on a single virtual superloop for an Option 11C/11C-Mini, for a maximum number of 640 VTNs in each system.

In Option 11C/11C-Mini, mapping virtual superloops to virtual cards is the same as mapping phantom superloops to phantom cards (see Table 59 on page 261).

Table 59
Virtual superloop/virtual card mapping for Option 11C/11C-Mini

SUPL	Card
96	61-64
100	65-68
104	69-72
108	73-76
112	77-80

Succession CSE 1000 Rel 2.0

Table 60 on page 262 lists the virtual superloop and virtual card mapping for the Succession CSE 1000 Rel 2.0 system.

Table 60
Virtual superloop/virtual card mapping for Succession CSE 1000 Rel 2.0

SUPL	Card	
96	61-64	81-84
100	65-68	85-88
104	69-72	89-92
108	73-76	93-96
112	77-80	97-99

LD 97 PRT TYPE SUPL prints the implicit virtual, phantom, or DECT cards for a virtual, phantom, or DECT superloop.

LD 21 LUU allows the user to list unused units of a specified type (iset, vtrk, phantom, DECT in a specified range of (virtual, and so on) TNs. Similarly, LUC of a specified type (virtual, phantom, or DECT) prints a list of unused cards on configured superloops.

Configure Internet Telephone features (LD 11)

The existing ISM header that is printed at the start of LD 11 includes the new ISM limit for the Internet Telephone. Refer to Table 46 on page 210 to configure the i2002 Internet Telephone, i2004 Internet Telephone, or the i2050 Software Phone in LD 11.

Table 61
LD 11 Configure an Internet Telephone (Part 1 of 2)

Prompt	Response	Description
REQ:	 NEW CHG PRT OUT CPY MOV	Action request. New Change Print Out Copy Move
TYPE:	I2002 I2004 I2050	For model i2002 Internet Telephone, i2004 Internet Telephone or i2050 Software Phone. Meridian 1 and Succession CSE 1000 accepts this response if it is equipped with packages 88 and 170. The i2002 and i2050 are also restricted by the Internet Telephone ISM setting.
TN	l s c u c u	Enter loop (virtual loop), shelf, card, and unit (terminal number), where unit = 0 - 31 Slot (virtual slot) and unit for Option 11C. ***Note:*** See Table 59 on page 261 for virtual superloop to virtual card slot mapping for Option 11C/11C-Mini.
DES	a...z	ODAS telephone designator.
CUST	0-99	Customer number.

Table 61
LD 11 Configure an Internet Telephone (Part 2 of 2)

Prompt	Response	Description
ZONE	0-255	Zone number to which this Internet Telephone belongs. The zone prompt is applied only when TYPE = i2002, i2004, or i2050. ***Note:*** Verify that the zone number exists in LD 117.
CLS	aaaa	ADD - Automatic Digit Display, default for Internet Telephone. For a complete list of responses, refer to *Software Input/Output: Administration* (553-3001-311).
KEY	xx aaa yy zz...zz	Telephone function key assignments where: xx = Keys 0 - 5 (and 6 - 11 using Shift key) for i2004 and xx = Keys 0 - 3 for the i2002. These are self-labeled physical keys that can be programmed with any feature. aaa = Key name or function yyy, zzz = additional information required for the key. ***Note:*** Keys 16 - 26 are reserved for dedicated Internet Telephone soft keys. Table 62 lists the dedicated Internet Telephone key name values (aaa). Other key name values can be found in *Software Input/Output: Administration* (553-3001-311).

Internet Telephone dedicated soft keys

Table 62 on page 265 describes the Meridian 1 and Succession CSE 1000 features that can be assigned to dedicated soft keys 16-26 on the i2002 Internet Telephone, i2004 Internet Telephone, or i2050 Software Phone. Remove unused feature keys by configuring the dedicated soft keys to NUL. Some features depend on the given Class of Service.

If an attempt is made to configure anything other than the permitted response, Meridian 1 and Succession CSE 1000 generates an error code. For related error messages, see SCH messages in *Software Input/Output: System Messages* (553-3001-411).

Table 62
LD 11 Internet Telephone dedicated soft key assignment (Part 1 of 2)

Internet telephone key number	Response(s) Allowed
Key 16	MWK, NUL MWK - Message Waiting key
Key 17	TRN, NUL TRN - Call Transfer key
Key 18	A03, A06, NUL AO3 - 3-party conference key AO6 - 6-party conference key
Key 19	CFW, NUL CFW - Call Forward key
Key 20	RGA, NUL RGA - Ring Again key
Key 21	PRK, NUL PRK - Call Park key

Table 62
LD 11 Internet Telephone dedicated soft key assignment (Part 2 of 2)

Internet telephone key number	Response(s) Allowed
Key 22	RNP, NUL RNP - Ringing Number pickup key
Key 23	SCU, SSU, SCC, SSC, NUL SCU - Speed Call User SSU - System Speed Call User SCC - Speed Call Controller SSC - System Speed Call Controller
Key 24	PRS, NUL PRS - Privacy Release key
Key 25	CHG, NUL CHG - Charge Account key
Key 26	CPN, NUL CPN - Calling Party Number key

Configuration of IP Telephony Nodes using OTM 2.0

Contents

This section contains information on the following topics:

Reference list

The following are references for this section:

- *Internet Terminals Description* (553-3001-217)
- *Installing and Configuring Optivity Telephony Manager* (553-3001-230)
- *Using Optivity Telephony Manager* (553-3001-330)
- *Upgrades* (553-3023-258)

Overview

This chapter explains how to configure IP Telephony nodes and Voice Gateway Media Cards using Optivity Telephony Manager (OTM).

This chapter also provides instruction for transmitting data to Voice Gateway Media Cards; upgrading card loadware; and upgrading i2004 Internet Telephone firmware using OTM.

Read the “IP Network Engineering Guidelines” on page 133 before installing an IP Telephony node.

Configure IP Line data using OTM

Optivity Telephony Manager (OTM) can be used to manually add and configure IP Telephony nodes. OTM 2.0 includes a new IP Line 3.0 application that is used to configure nodes on Meridian 1 or Succession Communication Server for Enterprise (CSE) 1000 Rel 1.1 systems. Multiple IP Telephony nodes for Internet Telephones are configured and managed from the same OTM PC.

A node is defined as a collection of Signaling Servers and Voice Gateway Media Cards (ITG-P Line Cards and Succession Media Cards). Each node in the network has a unique Node ID. This Node ID is an integer value. A node has one and only one primary or Leader Voice Gateway Media Card. All the other Voice Gateway Media Cards are defined as Followers.

> ***Note 1:*** All IP addresses and subnet mask data must be in dotted decimal format. Convert subnet mask data from Classless Inter-Domain (CIDR) format.

> ***Note 2:*** Refer to the Table 45 on page 209 and for IP addresses and information required in this procedure.

WARNING

OTM 2.0 does not support configuration of nodes which reside on a Succession CSE 1000 Rel 2.0 system. However, since OTM is required for retrieval of Operational Measurement (OM) reports from nodes on these systems, OTM is capable of being configured with basic network connection information of the node. The necessary configuration to retrieve the OM reports is covered in Procedure 14 through Procedure 18. In these procedures, pay special attention to any comments specific to nodes which reside on a Succession CSE 1000 Rel 2.0 system.

Launching OTM and the IP Line 3.0 application

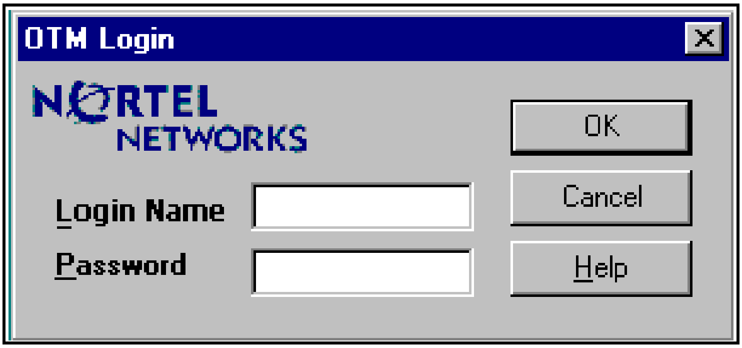
To launch the Optivity Telephony Manager and start the IP Line 3.0 application, perform the steps in Procedure 14 on page 270.

Procedure 14
Launching OTM

1 Select **Start | Programs | Optivity Telephony Manager | OTM Navigator**.

2 The **OTM Login** screen appears (see Figure 29 on page 270). Enter the **Login Name** and **Password**. Click **OK**.

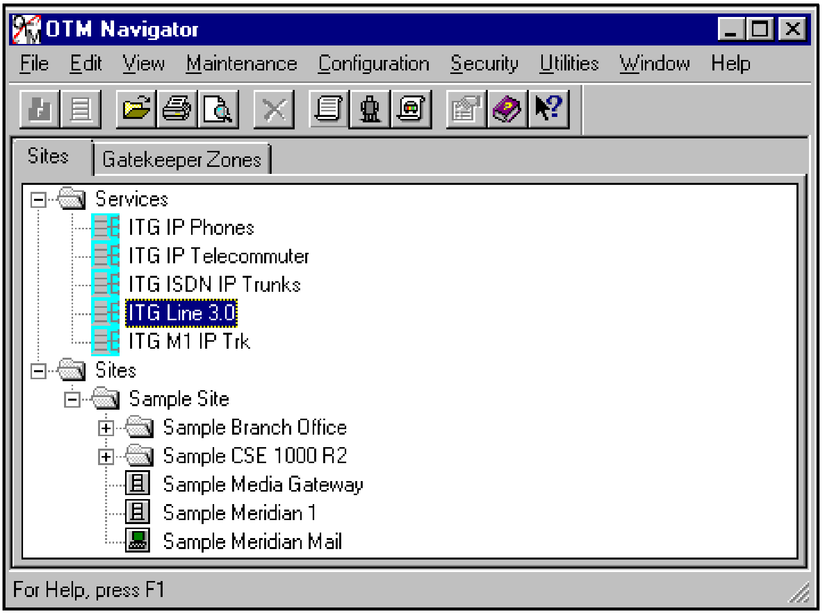
Figure 29
OTM Login screen



3 The OTM Navigator window opens. OTM Navigator has two tabs: Sites and Gatekeeper Zones. The IP Line 3.0 application that is available with OTM is located on the Sites tab. Click the **Sites** tab.

4 Expand the Services folder. Double-click the **ITG Line 3.0** icon to launch the IP Line 3.0 application (see Figure 30 on page 271). The **IP Telephony Gateway - IP Line 3.0** window opens. This application is used to configure and administer the IP Telephony nodes and the Voice Gateway Media Cards.

Figure 30
OTM Navigator



End of Procedure

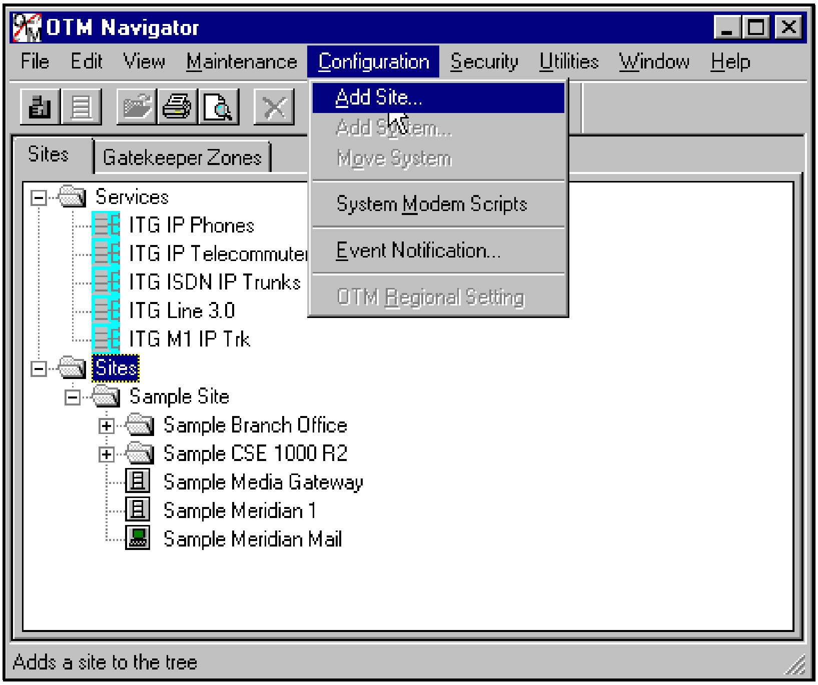
Adding a site, system, and customer

A site, system, and customer must be added before nodes and Voice Gateway Media Cards can be configured. Follow the steps in the following procedure to add a site, system, and customer using OTM Navigator.

Procedure 15
Adding a site, system, and customer

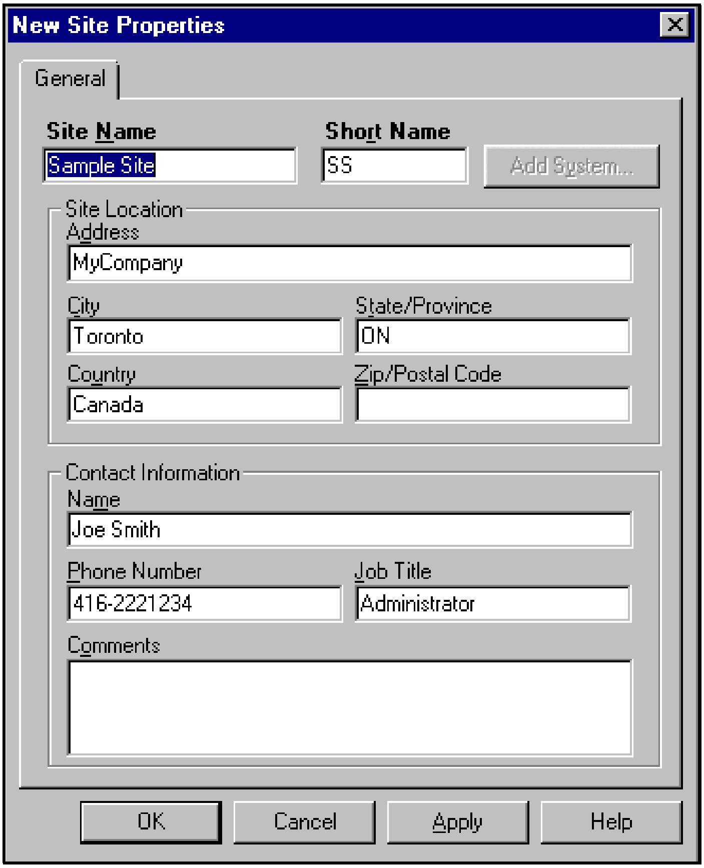
1 In the **OTM Navigator** window, click **Configuration | Add Site** (see Figure 31).

Figure 31
OTM Navigator–Configuration | Add Site



2 The **New Site Properties** window opens (see Figure 32 on page 273).

Figure 32
New Site Properties



3 In the **New Site Properties** window, set the following:

a. Site Name: Enter the name of the site.

b. Short Name: Enter a short name for the site.

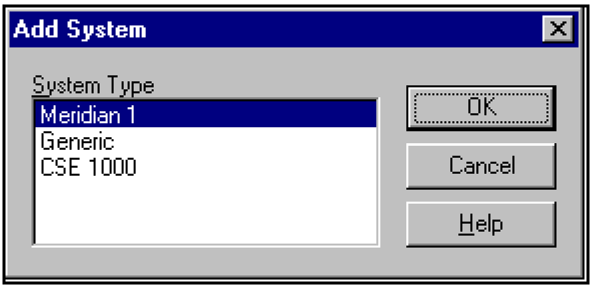
Under **Site Location**, add the **Address**, **City**, **State/Province**, **Country**, and **Zip/Postal Code** of the site.

Under **Contact Information**, add the **Name**, **Phone Number**, **Job Title**, and any **Comments** for the site contact person(s).

4 Click **Apply**. The **Add System** button (located in the upper right corner of the New Site Properties window) is enabled.

5 Click the **Add System** button. The **Add System** dialog window appears (see Figure 33).

Figure 33
Add System



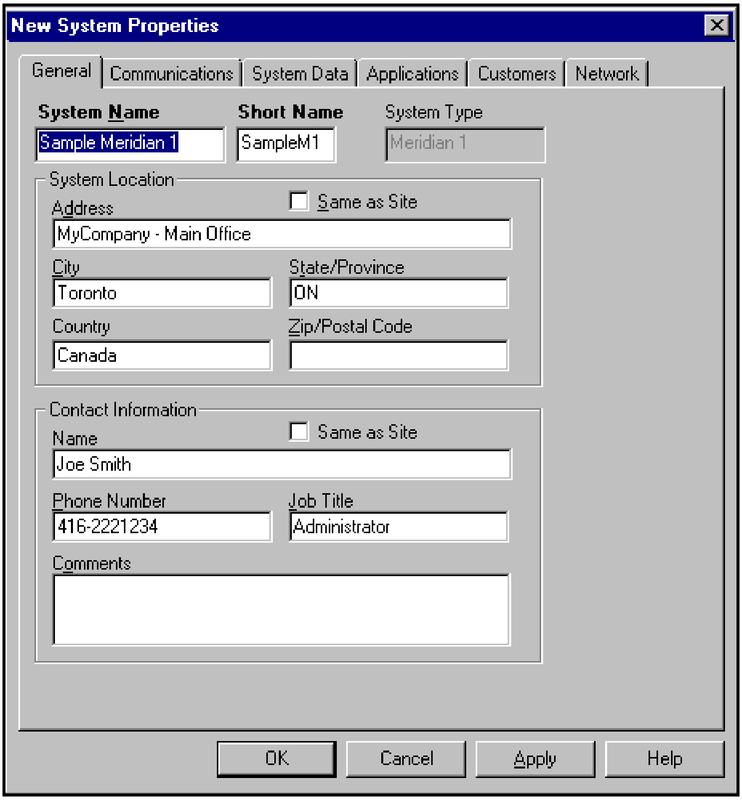
6 In the Add System window, select **Meridian 1** and click **OK**.

Note 1: To configure a Succession CSE 1000 Release 1.1 system, click Meridian 1.

Note 2: The only time a user should select CSE 1000 is when adding a Succession CSE 1000 Rel 2.0 to OTM.

7 The **New System Properties** window opens (see Figure 34 on page 275).

Figure 34
New System Properties



8 In the **New System Properties** window, set the following:

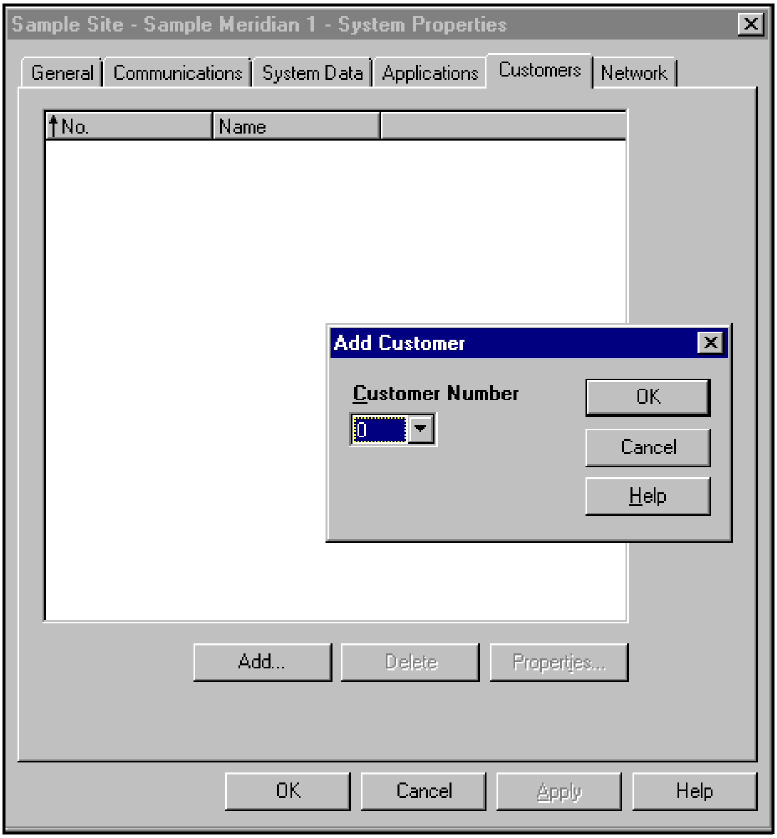
a. **System Name:** Enter the name of the system.

b. **Short Name:** Enter a short name for the system.

9 Click **Apply**. The **System Properties** window opens.

10 Click the **Customers** tab and then click the **Add** button. The **Add Customer** dialog window appears (see Figure 35 on page 276).

Figure 35
Add Customer



11 Select the **Customer Number** and click **OK**. This adds a customer to the system and opens the **New - (Customer n) Properties** window. Click **OK**. The System Properties window opens. Click **OK** to save and close the System Properties.

Note: Only the Customer Number is required to add a system. There is no need to enter any other customer data. The other data in the Customer tab and other System Properties tabs is not required for the IP Line 3.0 application. This data is used by other OTM applications.

End of Procedure

The following summary of steps are required to configure a Voice Gateway Media Card using OTM:

1. "Manually adding an IP Telephony node" on page 278.
2. "Configuring the card properties of the Voice Gateway Media Card" on page 282.
3. "Configuring DSP profile data" on page 284.
4. "Configuring SNMP traps and ELAN GW Routing table" on page 288.
5. "Configuring the Call Server ELAN IP address (Active ELNK) and the TLAN voice port" on page 292.
6. "Configuring security for SNMP access" on page 295.
7. "Configuring File Server access" on page 296.
8. "Configuring QoS support" on page 298.

Manually adding an IP Telephony node

Procedure 16
Adding an IP Telephony node manually

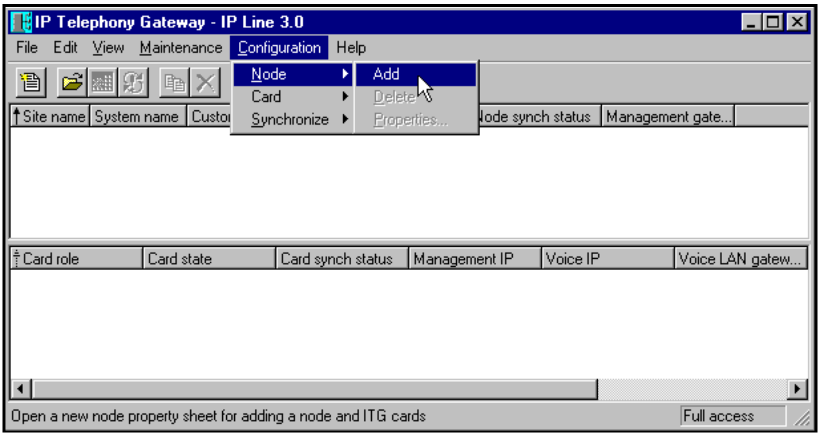
1 In the OTM Navigator window, click on the **Services** folder.

2 Double-click **ITG Line 3.0** icon (see Figure 30 on page 271).

3 The **ITG Telephony Gateway - IP Line 3.0** window opens.

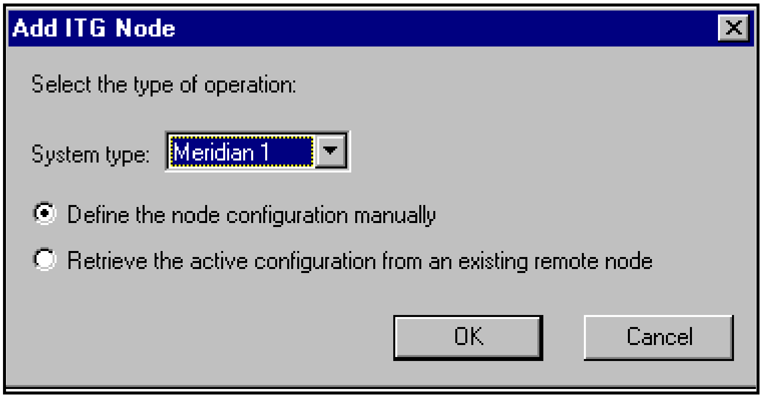
4 Click **Configuration | Node | Add** (see Figure 36 on page 278). The **Add Node** dialog box opens.

Figure 36
ITG Telephony Gateway - IP Line 3.0 main window



5 The **Add ITG Node** window opens (see Figure 37). Ensure the "Define node configuration manually" radio button is selected. Click **OK** to accept the default setting.

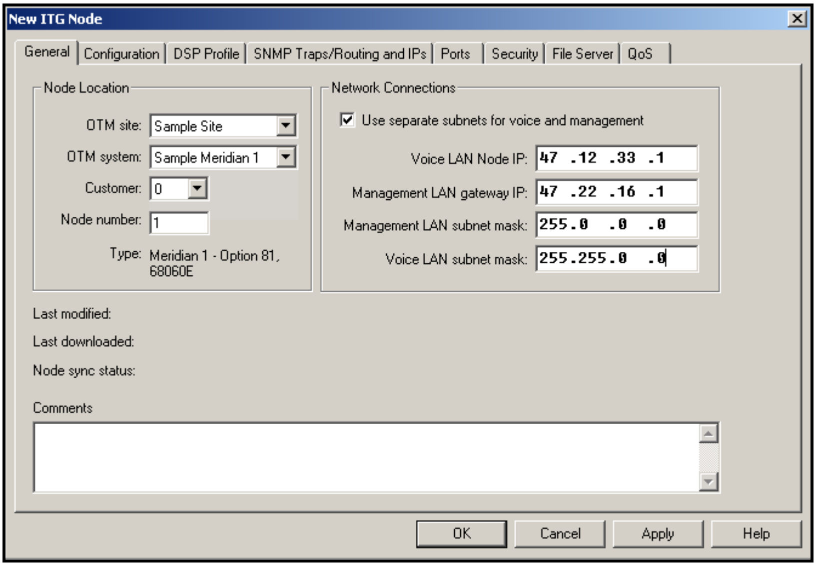
Figure 37
Add ITG Node



Note: The System type selection is always Meridian 1, even if a node which resides on a Succession CSE 1000 Rel 2.0 system is being added to the OTM database.

6 The **New ITG Node** window opens (see Figure 38 on page 280).

Figure 38
New ITG Node–General tab



7 On the **General** tab, under **Node Location**:

a. Select an **OTM site**, **OTM system**, and **Customer** number.

b. Type in a **Node number** (one to four digits). The Node Number field in the tab corresponds to the Node ID field in the Internet Telephone configuration.

CAUTION

The Voice Gateway Media Cards identify themselves with a node using the node number. If there are multiple IP Telephony nodes sharing the same TLAN, each node must have a unique id. Each system on the TLAN must have a unique node id assigned to the Voice Gateway Media Cards on the system.

c. Write down the node number, which is used in the Internet Telephone configuration.

8 Under **Network Connections**:

a. For IP Line 3.0, ensure the **Use separate subnets for voice and management** check box is selected.

> **CAUTION**
> The separate subnets option must be used in the TLAN and ELAN configuration.

b. **Voice LAN Node IP:** Enter the Voice LAN (TLAN) Node IP address in dotted decimal format. Press the space bar to move between each decimal point. The Voice LAN Node IP is on the TLAN. The Node IP address is the IP address used by the Internet Telephones to communicate with the Voice Gateway Media Cards on the TLAN. If a Voice Gateway Media Card becomes the primary (Leader) during an election, it assigns itself the Node IP address.

c. **Management LAN gateway IP:** Enter the Management LAN (ELAN) gateway IP address in dotted decimal format. This is the IP address of the gateway of the subnet to which the Voice Gateway Media Card belongs. This is the IP address of the router interface on the ELAN, if present. If there is no management LAN gateway, enter 0.0.0.0.

d. **Management LAN subnet mask:** Enter the Management LAN subnet mask address in dotted decimal format. This is the subnet mask that is used along with the ELAN IP address to identify the subnet to which the Voice Gateway Media Card belongs.

e. **Voice LAN subnet mask:** Enter the Voice LAN subnet mask address in dotted decimal format. This is the subnet mask used along with the TLAN IP address, to identify the subnet to which the Voice Gateway Media Card belongs.

9 Click the **Configuration** tab and continue with Procedure 17 on page 282.

End of Procedure

Configuring the card properties of the Voice Gateway Media Card

If the IP Network administrator provides IP addresses and subnet masks in CIDR format, for example, "10.1.1.10/24", convert the subnet mask to dotted decimal format. See Appendix D on page 675.

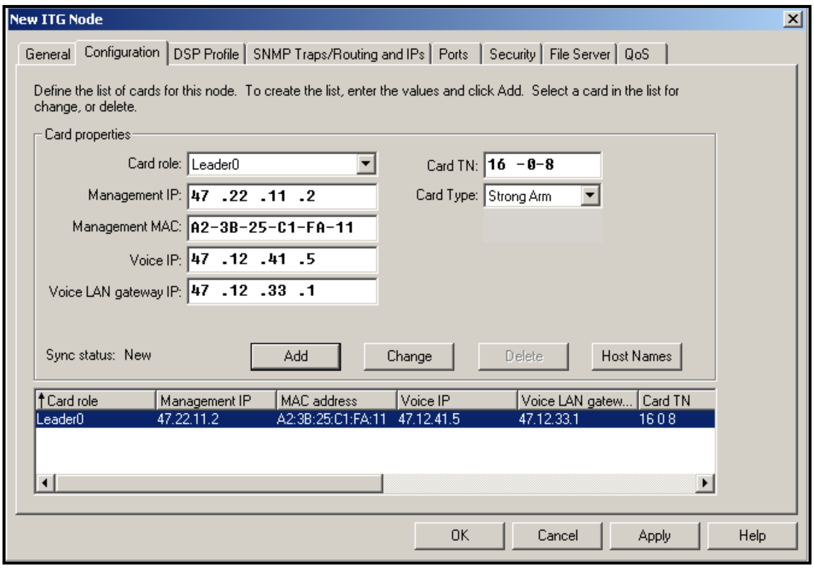
> ***Note 1:*** On the Configuration tab, cards can be Added, Changed, or Deleted in the node one at a time.

> ***Note 2:*** The Leader 0 card cannot be deleted in the Configuration tab. The node must deleted to delete Leader 0.

Procedure 17
Configuring the card properties for the Voice Gateway Media Card

1 Click the **Configuration** tab in the New ITG Node window (see Procedure 39 on page 282).

Figure 39
New ITG Node–Configuration tab



2 Enter the **Card Properties** data for Leader 0 and Follower cards:

a. **Card role:** Assign the Card role, Leader 0, to the first card configured. Assign the second card configured as Leader 1 and all remaining cards as Follower.

Note: When adding cards for a node which resides on a Succession CSE 1000 Rel 2.0 system for the purpose of retrieving OM reports, always assign the Signaling Server to be the Leader 0 card. A backup Signaling Server, if present, is assigned to be the Leader 1 card and all the Voice Gateway Media Cards in the node are assigned to be Follower cards. If no backup Signaling Server is present, assign one of the Voice Gateway Media Cards in the node to be the Leader 1 card.

b. **Management IP:** This is the ELAN IP address for the card. OTM and Meridian 1 use this address to communicate with the card.

c. **Management MAC:** This is the motherboard Ethernet address from your "Voice Gateway Media Card installation summary sheet" on page 209.

d. **Voice IP:** This is the TLAN IP address for the card.

e. **Voice LAN gateway IP:** This is the IP address of the router interface on the TLAN.

f. **Card TN:** For Option 51C/61C/81/81C systems, enter Card TN (l s c) information. For Option 11C, 11C-Mini, and Succession CSE 1000 systems, enter two zeros followed by the card slot number (1-50). For example, 0 0 49. The card TN format is determined by the Meridian 1 and Succession CSE 1000 Release 1.x system type that is configured in the OTM Navigator. Ensure the correct system type is entered in the OTM Navigator before adding the node.

g. **Card Type:** Choose either Pentium or Strong Arm. Select Pentium if using the ITG-P Line Card (dual-slot card). Select Strong Arm if using the Succession Media Card (single-slot card).

h. Click **Add**. The card role and address information appears in a working list at the bottom of the New ITG Node window.

i. Repeat the above steps for each card that is being added to the node.

3 Click **Apply** to add the card(s) to the Node.

Note: When Apply is clicked, the title of the window changes from New ITG Node to ITG Node Properties.

End of Procedure

Configuring DSP profile data

In OTM, the DSP Profile tab and its two sub-tabs (**General** and **Codec Options**) are used to configure DSP profile data in OTM.

Follow the steps in Procedure 18 on page 285 to configure DSP profile data.

WARNING

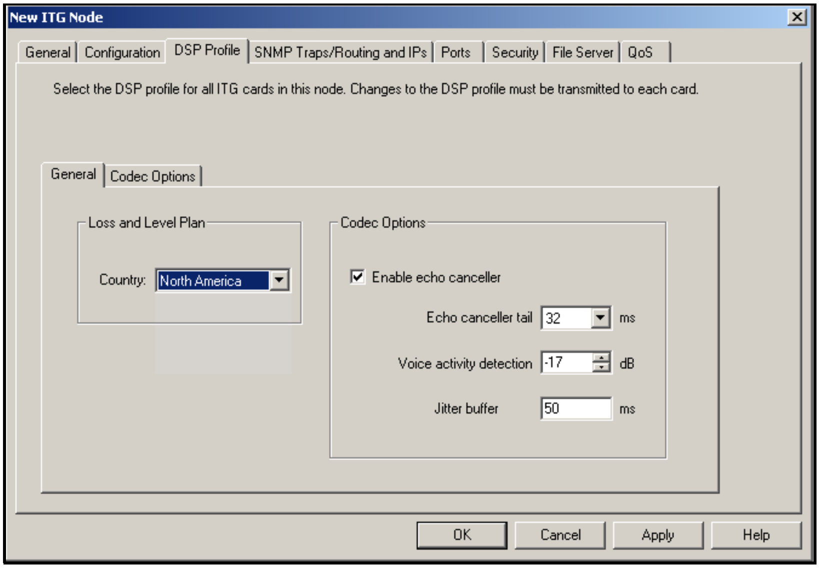
In order to add a node which resides on a Succession CSE 1000 Rel 2.0 system into the OTM database, it is necessary to first select a Loss and Level Plan. This step is necessary because selection of a Loss and Level Plan in OTM is mandatory prior to saving the node configuration into the OTM database.

The country selected for the Loss and Level Plan is inconsequential in this instance because the configuration is being saved for the sole purpose of allowing retrieval of Operation Measurement (OM) reports. Once a Loss and Level Plan has been selected, click the OK button to close the window and then exit Procedure 18.

Procedure 18
Configuring DSP profile data using OTM

1 Click the **DSP Profile** tab. The DSP Profile **General** sub-tab opens (Figure 40).

Figure 40
ITG Node Properties–DSP Profile tab–General sub-tab



2 Under **Loss and Level Plan**, select your **Country** from the pull-down box.

Loss and Level Plan determines parameters, such as transmission gain, that vary from country to country. The Loss and Level Plan values are stored in a file on the OTM PC. OTM reads the file to acquire the loss and level values for the selected country and places the values in a CONFIG.INI file on the Voice Gateway Media Cards.

3 Under **Codec Options**, leave the values at their default settings unless directed to change them as follows or by Nortel Networks Field Support.

a. Enable echo canceller: The echo canceller is enabled by default. Do not uncheck this box. Never disable echo canceller unless directed by Nortel Networks Field Support.

b. Echo canceller tail: Select the maximum value available. Never reduce the echo canceller tail delay value unless directed by Nortel Networks Field Support.

c. Voice activity detection: The default value is -17. The range is -20 to +10 dB.

d. **Jitter buffer:** The jitter buffer range is 0-200 ms and this range is determined by the codec. The default is 50 ms or the next highest setting that the device allows. For more information, see "Adjusting jitter buffer size" on page 189.

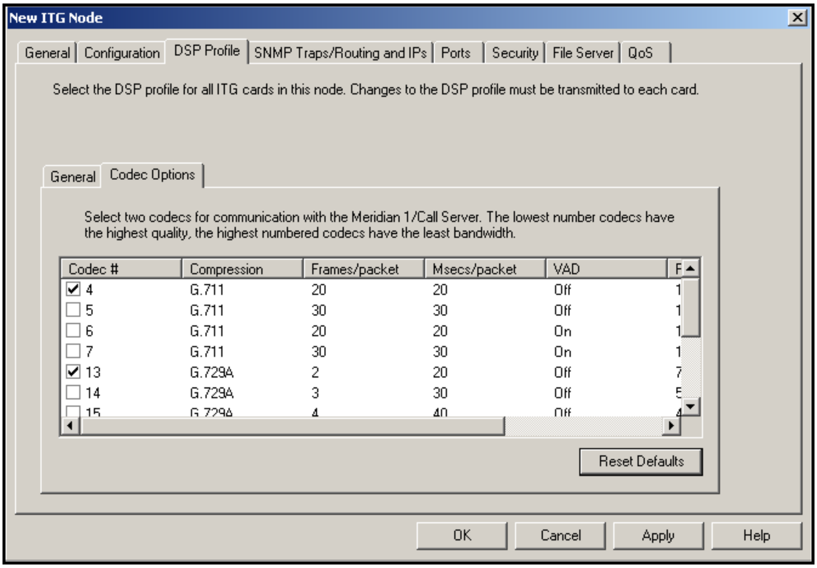
4 Click **Apply**.

5 Click the **Codec Options** sub-tab (Figure 41 on page 287).

The Codec Options sub-tab presents a table of different sets of codec options identified by a codec setting index number. The lesser codec setting index corresponds to BQ (Best Quality) in LD 117 zone configuration. The greater codec setting index corresponds to BB (Best Bandwidth). For more information, see"Codec selection" on page 191.

Note: The Codec Options sub-tab contains a list of up to 32 codec settings for G.711, G.729A, and G.729AB for the Voice Gateway Media Card (see Figure 41 on page 287).

Figure 41
ITG Node Properties–DSP Profile tab–Codec Options sub-tab



6 Check exactly two **Codec #** settings from the list. The Codec # indicates a particular codec (G.711, G.729A, G.729AB) with different options for Frame Size and VAD (On or Off). The default Codec # settings are 4 and 17. The lessor of the two Codec #s that is checked corresponds to BQ (best quality) and BB (best bandwidth) in LD 117.

For example, if Codec # 4 and Codec # 13 are selected:

- Codec # 4 corresponds with best quality
- Codec # 13 corresponds with best bandwidth

Note: If there are multiple nodes on a system and the same codec is selected on more than one node, ensure that each node has the same voice payload size configured for the codec.

7 Click **Apply**.

End of Procedure

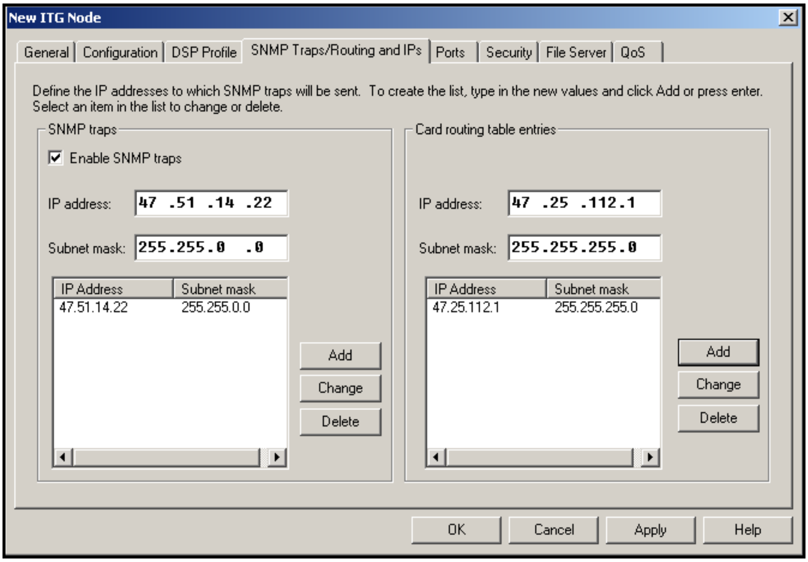
Configuring SNMP traps and ELAN GW Routing table

Procedure 19
Configuring SNMP traps and ELAN GW Routing table

1 Click the **SNMP Traps/Routing and IPs** tab in the ITG Node Properties window (see Figure 42).

IP addresses that are added in this tab create special card routing tables that direct packets out the ELAN and ELAN gateway. Exercise caution when adding entries since the entry could result in one-way voice transmission if a change results in voice packets being streamed out the ELAN instead of the TLAN interface.

Figure 42
ITG Node Properties–SNMP Traps/Routing and IPs tab



2 Under **SNMP traps**:

   a. **Enable SNMP traps:** Check the Enable SNMP traps checkbox, if configuring one or more SNMP management IP addresses to receive SNMP traps from cards in the IP Telephony node.

   b. **IP address:** If SNMP traps are enabled, the SNMP traps are sent to the IP address entered here.

   c. **Subnet mask:** If SNMP traps are enabled, this is the subnet mask where SNMP traps are sent.

   To add an SNMP Manager IP address, type the IP address in the SNMP traps entry fields, and click **Add**. Add SNMP Manager IP addresses for:

   — the local or remote OTM server

   — PPP IP address configured in the Netgear RM356 Modem Router, or equivalent, on the ELAN for the remote support OTM PC

   — the SNMP manager for remote alarm monitoring

Note 1: Up to eight SNMP trap servers can be defined.

Note 2: A net route or host route through the management gateway is added to the Voice Gateway Media Cards IP Routing Table for each SNMP management address that is added to the SNMP traps list.

3 Under **Card routing table entries**, enter the **IP address** and **Subnet mask** for any host that is not on the ELAN subnet but requires access to the Voice Gateway Media Card across the ELAN. A Telnet session for maintenance from a remote PC is an example of when this would be needed. The address of the remote PC would be added in the Route list.

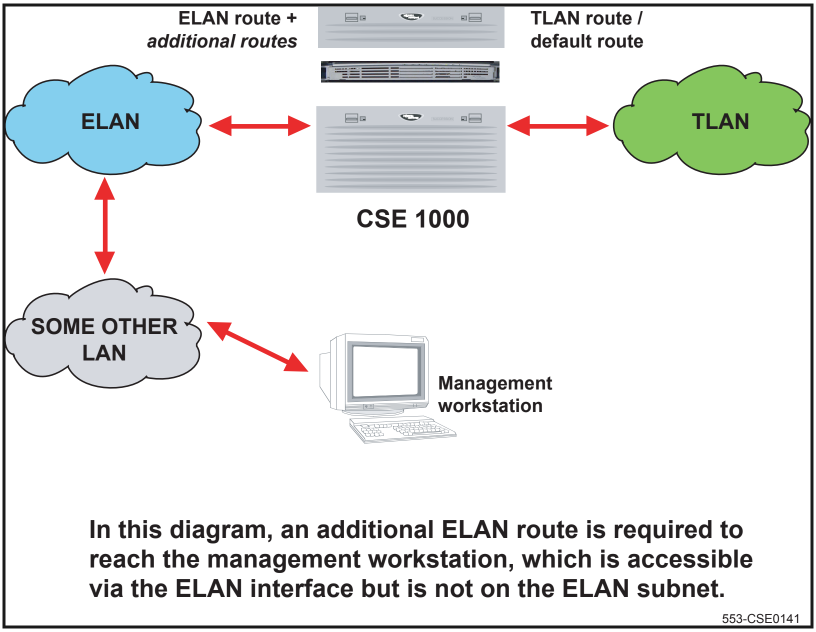
The default route on the card causes packets for unknown subnets to be sent out the TLAN interface. Packets from an external host arrive on the ELAN interface and responses are sent on the TLAN interface. This can cause one way communication if the TLAN is not routed to the ELAN. It is necessary to add an entry in the Route list, to correct the routing so response packets are sent on the ELAN. Each entry creates a route entry in the card's route table that directs packets out the ELAN interface (see Figure 43 on page 291).

CAUTION
Use caution when assigning card routing table entries. Do not include the IP address of an Internet Telephone. Otherwise, voice traffic to these Internet Telephones is incorrectly routed through the ELAN and ELAN gateway. To avoid including the wrong IP address, Nortel Networks recommends that Host IDs are defined for the card routing table entries.

To add a net route or host route, type the IP address and subnet mask in the entry field of the card routing table, and click **Add**.

4 Click **Apply**.

Figure 43
Specifying additional ELAN routes



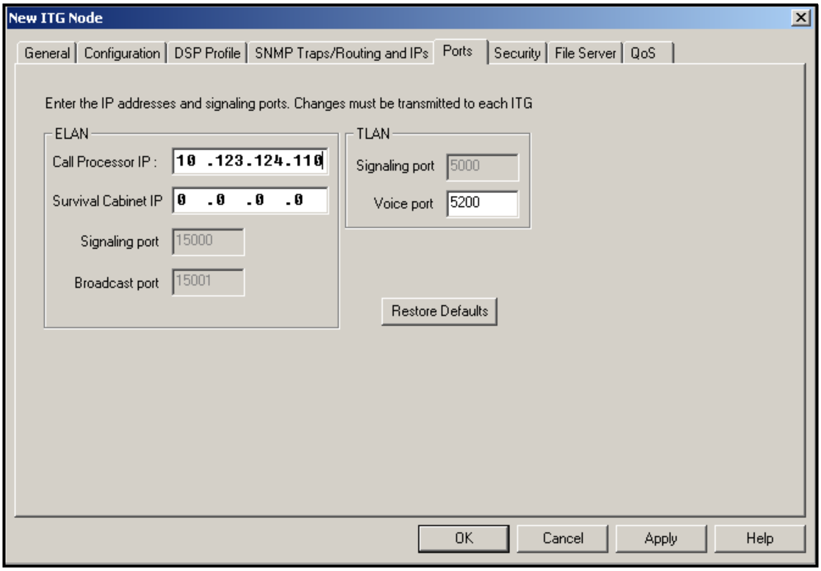
End of Procedure

Configuring the Call Server ELAN IP address (Active ELNK) and the TLAN voice port

Procedure 20
Configuring the Call Server ELAN IP address (Active ELNK) and the TLAN voice port

1 Click the **Ports** tab (Figure 44).

Figure 44
ITG Node Properties–Ports tab



2 Enter the following **ELAN** settings:

a. **Meridian 1 IP:** Enter the Meridian 1 ELAN IP Address (Active ELNK).

Note: The Meridian 1 ELAN IP address must correspond to the Active ELNK IP address configured in LD 117. It must be in the same subnet as the ELAN for the IP Telephony node.

b. **Survival Cabinet IP:** If applicable, enter the Survivable Cabinet ELAN IP address (Active ELNK). This is the IP address that is configured for survivability. The survivable Cabinet IP is enabled only for Option 11C and Succession CSE 1000 systems.

Note: For Option 11C, Option 11C-Mini, or Succession CSE 1000, this field is disabled unless you have defined at least one cabinet as a survival cabinet of the main system in OTM Navigator. There is only one survival cabinet IP address for each node. The survivable cabinet is equipped with sufficient Trunk cards and Voice Gateway Media Cards. In case of Call Server equipment failure, it provides a large degree of survivability for Internet Telephone users.

c. **Signaling port:** The default value is 15000. This field is read-only.

d. **Broadcast port:** The default value is 15001. This field is read-only.

3 Enter the following **TLAN** settings:

a. **Voice port**: Change the Voice port only as instructed by the IP network administrator to improve Quality of Service for the Internet Telephones. For example, if RTP Header compression is used to reduce voice bandwidth on narrow band WAN links, then TLAN voice port range must be set to 16384 or higher. The exact range will be provided by the system administrator.

Note 1: The TLAN Voice port range is 1024 to 65535. The default Voice ports are 5200-5295.

Note 2: The TLAN Signaling occurs on UDP ports 7300, 4100, 5100, and 5000.

> **CAUTION**
> Do not set the Voice port to a value that is already used for signaling (4100, 5000, 5100, 7300).
>
> The Voice port defines the first port in a range spanning the gateway channels on the card; this means a Voice port value of 5200 reserves ports 5200-5263 on the Succession Media Card and 5200-5247 on the ITG-P Line Card. If this value is changed from the default, confirm the selected Voice port value does not range into one of the reserved signaling port values.

4 Click **Apply**.

End of Procedure

Configuring security for SNMP access

Procedure 21 explains how to change the SNMP community names. This provides better security for the IP Telephony node. OTM uses the community name password to refresh the Voice Gateway Media Card status, and to control the transmitting and retrieving of configuration data files for database synchronization.

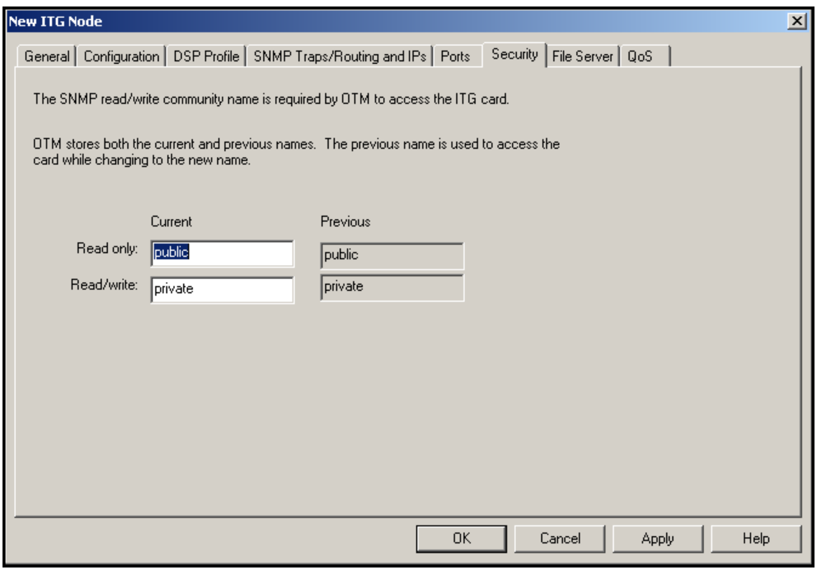
> *Note:* If the community names are forgotten, connect a TTY to the Voice Gateway Media Card maintenance port. Restart the card. The card displays the community name on the TTY during startup.

To configure the SNMP community names, follow the steps in Procedure 21 on page 295.

Procedure 21
Configuring security for OTM SNMP access

1 Click the **Security** tab (Figure 45).

Figure 45
ITG Node Properties–Security tab



2 Change the default **Read only** and **Read/write** community names.

OTM uses the **Previous Read/write** community name to transmit the card properties. The first time data is transmitted after changing the password, the Previous Read/write password is used. For all following data transmissions, the changed password is used.

3 Click **Apply**.

End of Procedure

Configuring File Server access

With the addition of new Internet Telephones, there are also additional firmware files for the Internet Telephones. The Voice Gateway Media Card has limited space to store the files on the card for all the telephones. As a result, a file server can be used to store the telephone firmware files.

The i2004 Internet Telephone firmware filename 0602Bnn.BIN where Bnn = F/W version 1.nn.

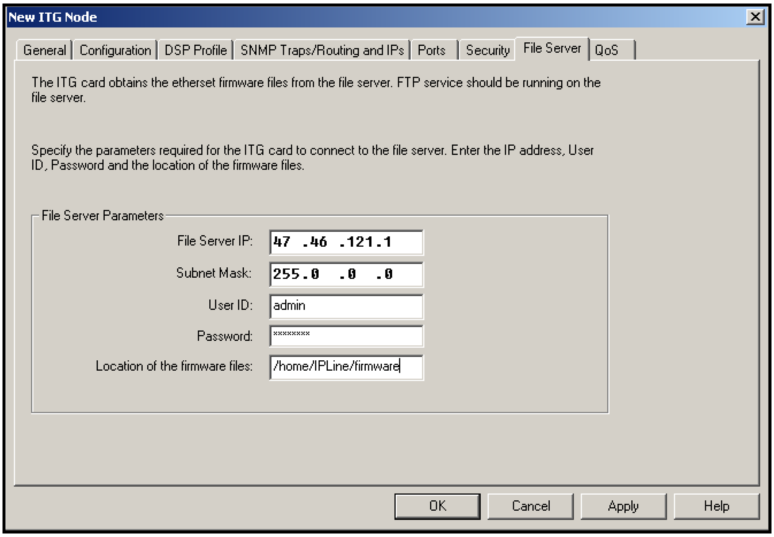
If the external file server option is used in OTM for firmware distribution with a node, the 0602Bnn.BIN file must be renamed to i2004.fw before being placed on the server.

To configure the file server, follow the steps in Procedure 22 on page 297.

Procedure 22
Configuring access to the File Server

1 Click the **File Server** tab (Figure 46).

Figure 46
ITG Node Properties–File Server tab



2 Under **File Server Parameters**, specify the parameters needed to connect to the file server:

a. **File Server IP:** Enter the IP address of the file server.

b. **Subnet Mask:** Enter the Subnet Mask of the file server.

c. **User ID:** Enter the User ID that is required to access the file server.

d. **Password:** Enter the Password that is required to access the file server.

e. **Location of the firmware files:** Enter the path for the location of the firmware files. See page 103 for the default location of firmware files for the Meridian 1 and Succession CSE 1000 Rel 2.0 systems.

3 Click **Apply**.

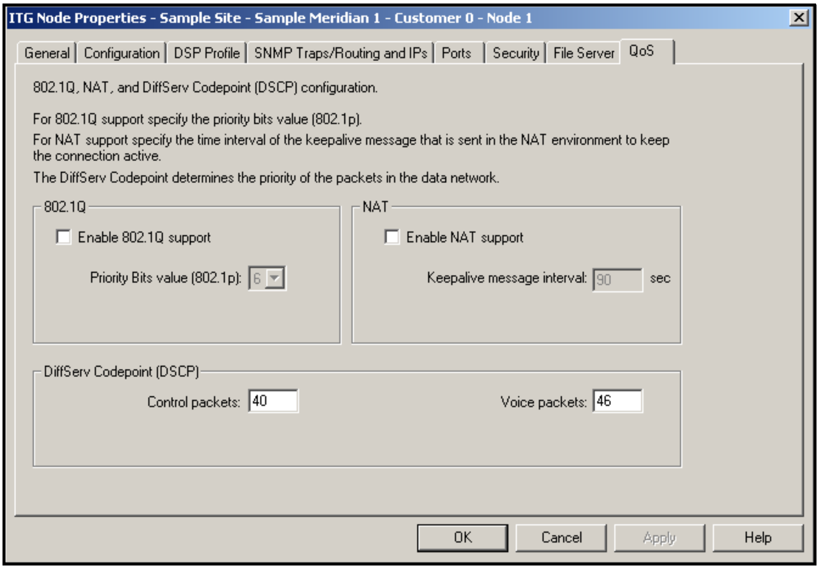
End of Procedure

Configuring QoS support

Procedure 23
Enabling 802.1Q support and NAT support, and configuring Diffserv Codepoint settings

1 Click the **QoS** tab (Figure 47).

Figure 47
ITG Node Properties–QoS tab



2 802.1Q enables virtual LANs (VLANs) to be defined within a single LAN. This improves bandwidth management and limits the impact of broadcast and multicast messages.

802.1Q settings:

a. **Enable 802.1Q support:** Check the check box to enable 802.1Q support. By default, 802.1Q support is disabled.

b. **Priority Bits value (802.1p):** The priority field is a 3-bit value, with a default value of 6. The range is 0-7. A value of 6 is recommended by Nortel Networks. The p bits within the 802.1Q standard enables packet prioritization at Layer 2 improving network throughput for IP Telephony data.

Note: These values are applied to all Voice Gateway Media Cards in the node.

3 NAT provides mapping of public to private addressing. Support for networks containing NAT devices has been enhanced with the addition of a periodic message that is sent to prevent the RTP packet stream's NAT session from timing out. This could occur when the Internet Telephone is muted and packet transmission is stopped.

NAT settings:

a. **Enable NAT support:** Click this check box to enable the periodic sending of the session Keep Alive message. By default, this is disabled and the message is not sent.

b. **Keepalive message interval:** The field defines the delay between transmissions of the dummy message. The default value is 90 seconds. The range is 30-120 seconds. Set this to a value that is shorter than the NAT device's session timeout value.

4 Under **Diffserv Codepoint**, modify the DSCP Control and Voice values only as directed by the IP network administrator.

The recommended configuration values are:

a. **Control packets:** A value of 40 - Class Selectore 5 (CS5). This sets the priority of the signaling messaging.

b. **Voice packets:** A value of 46 Control DSCP - Expedited Forwarding (EF).

DiffServ, the Differentiated Service (DiffServ) code point (DSCP) determines the priorities of the management and voice packets in the

IP Line network. The range for both management and voice packet DiffServ is 0-63 inclusive.

The DiffServ value can be configured, if required, to obtain better QoS over the IP data network (LAN/WAN).

The value entered depends on the policy in the customer's data network.

Note: Do not change DiffServ from the default values unless instructed below or by the IP network administrator.

5 Click **Apply** and then click **OK**.

End of Procedure

Transmit node configuration from OTM to the Voice Gateway Media Cards

Before beginning, ensure the:

- Voice Gateway Media Cards and cables have been installed.
- ELAN and TLAN interfaces of all cards are connected with access to the IP network.
- IP Line data has been configured in OTM.
- OTM server is connected to the local ELAN subnet or to a remote subnet with IP router access to the ELAN and TLAN.

Overview

The IP Telephony node and card properties are configured using OTM 2.0's IP Line 3.0 application. The configuration data is converted to text files by OTM and is then transmitted to Voice Gateway Media Cards.

The process consists of the following steps:

1 Set the Leader 0 IP address from TTY connected to local RS232 maintenance port.

2 Reboot Leader 0.

3 Transmit the node and card properties from the OTM IP Line 3.0 application to Leader 0.

4 Reboot Leader 0.

5 Transmit card properties to all cards in the node.

Setting the Leader 0 IP address

Follow the step in Procedure 24 to set the IP address of the Leader 0 Voice Gateway Media Card.

Procedure 24
Setting the Leader 0 IP address

1 Access the IPL> CLI by connecting the COM port of a OTM PC to the RS232 serial maintenance port on the faceplate of the Leader 0 Voice Gateway Media Card with an NTAG81CA PC Maintenance cable. If required, use an NTAG81BA Maintenance Extender cable between the PC Maintenance cable and the OTM PC.

Alternatively, connect the NTAG81BA Maintenance Extender cable to the female DB-9 connector of the NTMF94EA ELAN, TLAN RS232 Ports cable for a more permanent connection to the Voice Gateway Media Card serial maintenance port.

Note: Never connect two terminals to the faceplate and I/O panel breakout cable serial maintenance port connectors at the same time.

2 Use the following communication parameters for the TTY terminal emulation on the OTM PC: 9600 baud, 8 bits, no parity, one stop bit.

3 Login to the IPL> CLI and enter the **setLeader** command to set the Leader 0 Management LAN IP address, Management LAN gateway IP address and the Management LAN subnet mask.

4 Observe the Leader 0 card faceplate maintenance display window.

When the display reads "T:20", it begins to send BootP requests on the ELAN. A series of dots is printed on the TTY.

5 Type **+++** to escape from the BootP request.

6 At the Login prompt, enter the default user ID and password of **itgadmin** and **itgadmin** to access the IPL> CLI:

itg Login: itgadmin

Password: itgadmin

7 When the maintenance window displays "T:21", at the IPL> prompt, enter: **setLeader “xx.xx.xx.xx”,“yy.yy.yy.yy”,“zz.zz.zz.zz”**

Note 1: The three parameters must each be enclosed in double quotation marks. Ensure that there is a space after the command and before the first parameter. Put commas and no spaces between the following parameters:

“xx.xx.xx.xx”=IP address.
Enter the same IP address that was entered in the **Management LAN IP** field for **Leader 0** in the **Configuration** tab of the **ITG Node Properties**.

"yy.yy.yy.yy"=Gateway IP address.
Enter the same address that was entered in the **Management LAN gateway IP** field in the **General** tab of the **ITG Node Properties**. If there is none, enter the following: "**0.0.0.0**"

"zz.zz.zz.zz"=Management LAN subnet mask.
Enter the same address that was entered in the **Management LAN subnet mask** field in the **General** tab of the **ITG Node Properties**.

Note 2: This step assumes that the new IP Telephony node has already been configured in OTM.

8 Reboot the Leader 0 Voice Gateway Media Card. At the IPL> prompt, enter: **cardReset**, or press the Reset button on the faceplate of the Leader 0 Voice Gateway Media Card.

9 Check the maintenance display for T:22 to confirm a successful reboot.

10 From the OTM IP Telephony Gateway - IP Line 3.0 application, select **View | Refresh** to show the card status. Otherwise, verify LAN connections and IP configuration.

End of Procedure

Transmitting node and card properties to Leader 0

To transmit the node and card properties to Leader 0, follow the steps in Procedure 25.

> **CAUTION — Service Interruption**
>
> OTM does not support transmitting node and/or card properties to a node (or any of the card within the node) which resides on a Succession CSE 1000 Rel 2.0 system.

Procedure 25
Transmitting node and card properties to Leader 0

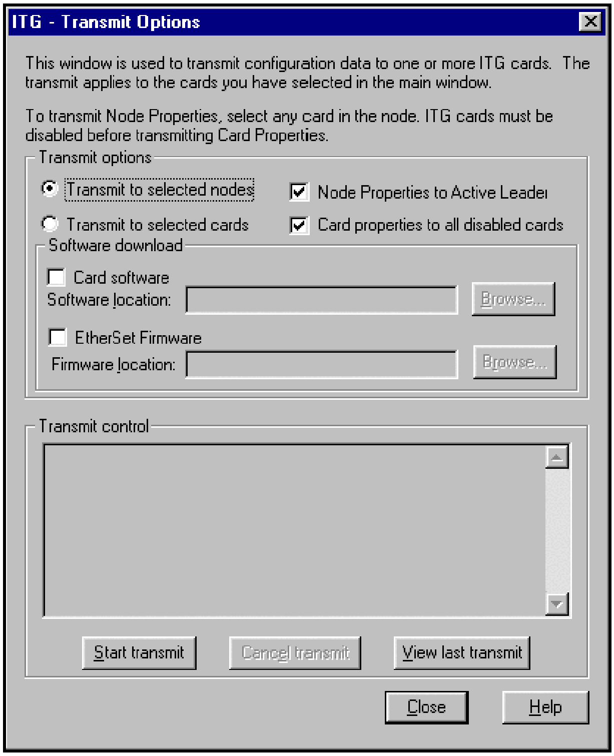
1 Login to LD 32 in Meridian 1. Disable the card in order to transmit the card properties.

2 Open OTM. From the **OTM Navigator** window, click on the **Services** folder to expand the menu. Double-click on **ITG Line 3.0**. The **IP Telephony Gateway - IP Line 3.0** window opens.

3 From the list of IP Telephony nodes in the upper part of the window, select the node to which configuration data is transmitted.

4 Select the **Configuration** | **Synchronize** | **Transmit**. The ITG - Transmit Options window appears (see Figure 48 on page 304).

Figure 48
ITG - Transmit Options dialog box



5 Use the default setting of **Transmit to selected nodes**. Check both the **Node Properties to Active Leader** and the **Card properties to all disabled cards** check boxes.

6 Click the **Start transmit** button. Monitor progress in the **Transmit control** area. Confirm that the node and card properties are transmitted successfully to Leader 0.

Note: At this point, it is normal that the card properties fail to transmit to the other cards in the node, because they have not yet received the IP address from Leader 0 BootP server.

7 When the transmission is complete, click **Close**.

8 Reboot the Leader 0 Voice Gateway Media Card. At the IPL> prompt, enter: **cardReset** or push the Reset button on the faceplate of the Voice Gateway Media Card.

End of Procedure

Transmitting card properties to all cards in the node

To transmit the card properties to all the Voice Gateway Media Cards in the node, follow the steps in Procedure 26.

> **CAUTION — Service Interruption**
>
> OTM does not support transmitting node and/or card properties to a node (or any of the card within the node) which resides on a Succession CSE 1000 Rel 2.0 system.

Procedure 26
Transmitting card properties to all cards in the node

To verify installation and configuration:

1 Check the displays on the card faceplate.

- After successfully rebooting, the Leader 0 card is now fully configured with the Node Properties of the node and enters a state of “active Leader”. The card faceplate display shows **Lxxx**, where xxx = the number of Internet Telephones registered with the terminal proxy server on the Leader card. L000 shows that no Internet Telephones are registered.

- The Leader 1 card, in OTM, and any Follower cards receive their configuration from the Leader 0 card. The faceplate display shows **Fxxx**, where xxx = the number of Internet Telephones registered with the Terminal Proxy Server on the Leader card. F000 shows that no Internet Telephones are registered.

2 Select the new IP Telephony node from the list in the upper part of the main window. All Voice Gateway Media Cards in the node are displayed in the lower part of the window.

3 While the node is selected, from the node list, press function key **F5** or select **View | Refresh | Selection** to refresh the card status of all cards in the selected node. The card status changes from "Unknown" or "Not responding" to "Disabled", "Enabled", and "Unequipped".

Note: If you are unable to communicate with Leader 1 and Followers in the node after transmitting the node properties and the card properties, and rebooting the Leader 0 card, this means that the Voice Gateway Media Cards are unable to communicate back to the remote OTM PC through the voice gateway or TLAN router.

To establish communication with the Leader 1 or other Follower cards in the IP Telephony node, perform the following:

a. Verify the TLAN physical and logical connections on all the non-responsive cards. Ensure that the:

i. cables are plugged securely into the correct TLAN connection

ii. switch is connected to correct TLAN router

iii. remote OTM can communicate with TLAN router

b. If remote OTM cannot communicate using the TLAN router, connect to the Voice Gateway Media Card maintenance port and use the IPL> CLI **routeAdd** command on each Voice Gateway Media Card to add a new IP route, through the management gateway that points to the remote OTM PC subnet.

c. Repeat step b, if the card is reset before OTM successfully transmits the card properties (containing the SNMP Manager IP addresses and the card routing IP addresses).

4 When Leader 1 and all Follower cards show a status of disabled, go into **Configure | Synchronize | Transmit**. When the Transmit window opens, click the **Transmit to selected nodes** radio button and the **Card properties to all disabled cards** check box to transmit the card properties.

5 Click **Start transmit**. Carefully monitor the progress to verify the card properties are successfully transmitted to every Voice Gateway Media Card in the selected node identified by its TN.

6 Verify that all Voice Gateway Media Cards in the node have established a signaling link to the Meridian 1 PBX CPU.

End of Procedure

Upgrade the Voice Gateway Media Card loadware and Internet Telephone firmware

Loadware refers to the software running on the Voice Gateway Media Cards in the Meridian 1 and Succession CSE 1000 systems.

Before upgrading the loadware and firmware, check the version of card loadware and Internet Telephone firmware that is currently installed. Compare this to the latest versions available by accessing the Nortel Networks Web site. Refer to Procedure 27 on page 309 for complete instructions.

When a loadware or firmware upgrade is required, go to the Nortel Networks Web site to download the appropriate upgrade files. When Internet access is unavailable from the OTM PC, use a PC with Internet access and transfer the files to the OTM PC for the following procedures.

i2004 Internet Telephone firmware requirements

The Internet Telephone has field upgradable firmware. With the introduction of IP Line 3.0, the number of Internet Telephones has increased. As a result of this increase there is also an increase in the number of firmware versions for the Internet Telephones. There is one firmware file for each type of Internet Telephone.

In the past, a copy of the firmware was stored on each card in the system to automatically upgrade Internet Telephones if an upgrade is required. There is limited space on the Voice Gateway Media Card (running IP Line 3.0) to store the firmware files. Therefore, the firmware is stored on a file server or on the Master card’s RAM device.

If a file server is used to store the firmware file, the following items are required to access the firmware:

- IP address of the file server
- Routing table
- File path to the file server
- User name and password required to access the files server

This information is configured in OTM IP Line 3.0 application. If using OTM, this information is configured in the File Server tab of the Node properties (see Figure 46 on page 297).

All i2004 Internet Telephones in a system must use the same version of firmware as the Voice Gateway Media Card.

The i2004 Internet Telephone uses Trivial File Transfer Protocol (TFTP) to transfer the firmware; therefore, the customer's network must support TFTP. For example, the customer's network cannot be blocked by a firewall.

CAUTION
The OTM PC should not be used as the file server for the firmware download.

Firmware upgrade from a new Voice Gateway Media Card

When the Voice Gateway Media Card is received from the factory, it has the latest i2004 firmware already installed in the C:/FW directory. As each i2004 Internet Telephone comes online, its firmware version is automatically compared to the version that is stored on the Voice Gateway Media Card. If they are different, the new firmware is downloaded from the Voice Gateway Media Card to the i2004 Internet Telephones. After the new firmware has been downloaded, the i2004 reboots and registers again with the Voice Gateway Media Card.

> ***Note:*** The i2004 Internet Telephone does not necessarily register with the same card as before the upgrade.

Verifying card loadware and Internet Telephone firmware

Before beginning, ensure that the following software is installed on the PC:

- Software to extract zipped files (WinZip or equivalent)
- A Web browser (such as Microsoft Internet Explorer or Netscape Navigator)

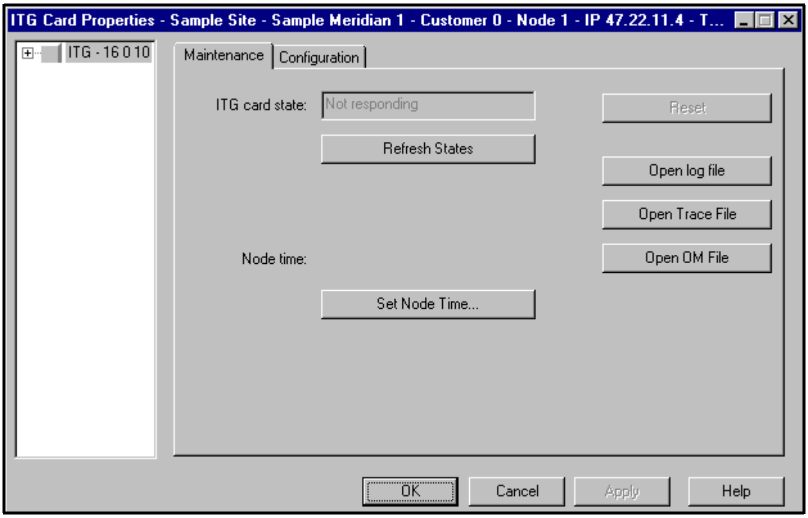
To verify the Voice Gateway Media Card loadware and the firmware on the i2004 Internet Telephone, follow the steps in Procedure 27.

Procedure 27
Verifying card loadware and Internet Telephone firmware using OTM

1 In the **OTM Navigator**, select the **Services** folder. Double-click on the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens. Select an IP Telephony node in the upper part of the window. A list of all line cards for that node appears in the lower part of the window.

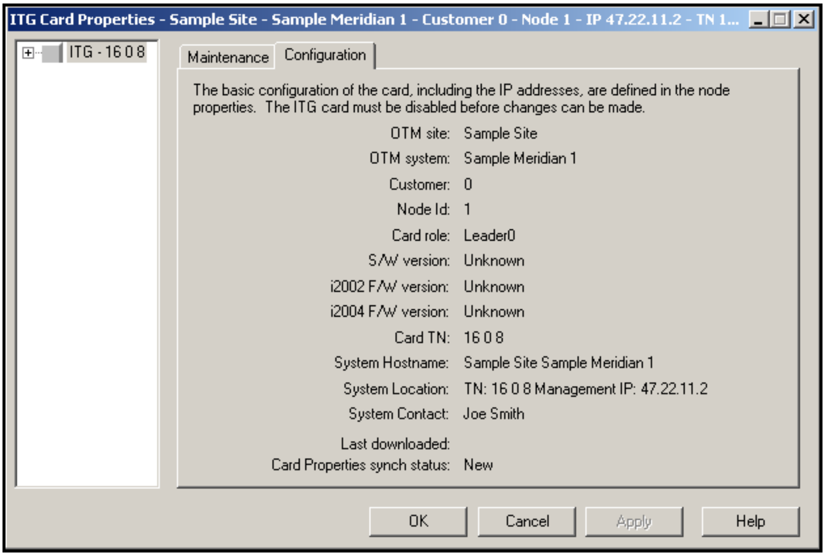
2 Starting with the Leader 0 Voice Gateway Media Card, double-click each Voice Gateway Media Card in the list to open the **ITG Card Properties** window. There are two tabs in the ITG Card Properties window: Maintenance and Configuration (see Figure 49 on page 310 and Figure 50 on page 311).

Figure 49
ITG Card Properties–Maintenance tab



3 Use the default settings in the Maintenance tab, and click the **Configuration** tab (see Figure 50 on page 311).

Figure 50
ITG Card Properties–Configuration tab



The current Voice Gateway Media Card loadware and Internet Telephone firmware versions are displayed on the Configuration tab. The Voice Gateway Media Card loadware is labelled **S/W version** and The Internet Telephone firmware is labeled **i2002** or **i2004 F/W version**.

4 Write down the loadware and firmware version for each Voice Gateway Media Card. Compare the loadware and firmware version with the latest recommended software release on the Nortel Networks Web site.

5 Check the Nortel Networks Web site for the latest IP Line 3.0 loadware and Internet Telephone firmware releases. Download the file. See Procedure 111 on page 719 for the steps for downloading files from the Nortel Networks Web site.

Note: The IP Line loadware and Internet Telephone firmware files are contained in the **IP Line 3.00.xx SA** file in the **Internet Telephony Gateway** product list on the Nortel Networks Web site. The zip file contains:

- The **IPL300xx*.p2** and **IPL300xx*.sa** loadware files. The IPL300xx*.p2 file is the IP Line application for the ITG-P Line Card and the IPL300xx*.sa is the IP Line application for the Succession Media Card.
- The **0602Bxx.BIN** (i2004) firmware file.

  For example, a firmware version can be labelled 0602B38. This means Internet Telephone firmware version 1.38.

  — The 02 represents the i2004 Internet Telephone.

  — The letter B represents the Version number 1.

  — 38 represents the Release number .38.
- A **readme.txt** file. The readme.txt file explains important considerations for installing the new loadware and firmware versions. The readme file also includes identifying information for the loadware and firmware files such as the date and time, size and checksum.

6 Locate the saved file and double-click the *.zip file. The zipped file opens in a compression utility program and the uncompressed files are listed.

7 If the card's loadware and firmware are not up-to-date, transfer the downloaded files (*.p2, *.sa, and firmware file(s)) from an Internet-enabled PC to the OTM PC.

8 If the card's loadware and firmware are not up-to-date, upgrade the Voice Gateway Media Card with the loadware and firmware files.

Refer to Procedure 28, "Upgrading Voice Gateway Media Card loadware from OTM PC" on page 314, and Procedure 30, "Upgrading the Internet Telephone firmware" on page 318 for detailed instructions on how to perform the upgrades.

Note: All cards must be running the same version of the loadware.

End of Procedure

Once the Voice Gateway Media Card loadware and i2004 Internet Telephone firmware has been verified, there are three upgrade options:

1 Upgrade the Voice Gateway Media Card loadware.
–In this case, perform Procedure 28 on page 314 only.

It may only be necessary to upgrade the Voice Gateway Media Card loadware. This option is used most frequently; however, verify if an Internet Telephone firmware upgrade is also required.

2 Upgrade both the Voice Gateway Media Card loadware and the i2004 Internet Telephone firmware.
–In this case, perform a combination of Procedure 28 and Procedure 30.

Both the Voice Gateway Media Card loadware and the i2004 Internet Telephone firmware may need to be upgraded.

Note: Defer restarting the cards until the end of Procedure 30, as restarting the cards restarts all the phones.

3 Upgrade the i2004 Internet Telephone firmware.
–In this case, perform Procedure 30 only.

It may only be necessary to upgrade the i2004 Internet Telephone firmware.

Note: In this case, restart all telephones instead of all cards. To do this, select a single test telephone and reset the software only on that test telephone before completing the procedure on all phones. If the upgrade works properly, use the umsUpgradeAll command to complete the upgrade on all the phones.

If the Voice Gateway Media Card firmware needs to be upgraded, follow the steps in Procedure 29 on page 317.

Upgrading Voice Gateway Media Card loadware

To upgrade the loadware on the Voice Gateway Media Card, follow the steps in Procedure 28 on page 314.

If Procedure 27 has just been completed, the correct loadware should have been verified and obtained for the Voice Gateway Media Card, and transferred the files to the OTM PC.

> *Note:* A node can contain a mix of ITG-P Line and Succession Media Cards. Each card type has a different loadware version. If a node contains a mix of cards, the loadware upgrade must be performed separately for each card type. That is, upgrade the ITG-P Line Card's loadware and then the Succession Media Card's loadware.

Procedure 28
Upgrading Voice Gateway Media Card loadware from OTM PC

1 Open the **OTM Navigator**, and click on the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.

2 Select the Voice Gateway Media Cards that are to be upgraded from the main card list view. Upgrade all the cards in the node together, unless a spare card that has older loadware is being installed.

3 Disable all Voice Gateway Media Cards to be upgraded. Use the Meridian 1 LD 32 DISI command from OTM Maintenance Windows, the OTM System Passthru terminal, or from a Meridian 1 system management terminal directly connected to a TTY port on the Meridian 1.

   Note: Nortel Networks recommends that a Voice Gateway Media Card be disabled prior to upgrading the loadware. However, it is possible to perform the transfer of the loadware to the card while the card is enabled. A Voice Gateway Media Card does not have to be disabled to transfer the loadware, however, the card must be disabled before it is rebooted.

4 In the **IP Telephony Gateway - IP Line 3.0** main window, select **View | Refresh** and verify that the card status is showing "Disabled."

5 Select **Configuration | Synchronize | Transmit**. The **ITG - Transmit Options** dialog box is displayed.

6 Under **Transmit options**, select the **Transmit to selected cards** radio button.

7 Under **Software download**, click the **Card software** check box.

8 Click on the **Browse** button to the right of the **Software location** text box.

9 Select the appropriate file filter (that is, ***.sa, *.p2, *.mms, *.***) from the **Files of type:** drop-down list box.

10 Locate the Voice Gateway Media Card loadware that was verified to be the correct version in Procedure 27 on page 309.

Select the file and click **Open** to save the selection. The path and file name of the Voice Gateway Media Card loadware appears in the **Software location** text box.

11 Click **Start transmit** to begin the Voice Gateway Media Card loadware upgrade process.

The loadware is transmitted to each card in turn, and burned into the flash ROM on the Voice Gateway Media Card.

12 Monitor progress in the **Transmit control** window. Confirm that the card loadware is transmitted successfully to all cards. Note any error messages, investigate and correct any problems, and repeat card loadware transmission until it is completed successfully on each Voice Gateway Media Card. The cards continue to run the old loadware until they are rebooted.

13 Reboot each Voice Gateway Media Card that received transmitted loadware. This enables the new loadware to take effect. Reboot Leader 0 first, followed by the other cards.

14 These cards must remain in the “Disabled” state after the upgrade, so that the technician can issue a “Reset” command from the Maintenance menu. Alternatively, click the Reset button on the Maintenance tab in the ITG Card Properties window of each card to reboot them. Also, the cards can be reset by using a pointed object to press the “Reset” button on the card faceplate.

WARNING
Do not use a pencil to reset the Voice Gateway Media Card. The graphite carbon can create an electrical short circuit on the board.

15 After all Voice Gateway Media Cards have been reset, have successfully rebooted, and are responding again to the OTM ITG Line Application, do a **Status refresh** (disabled: active; disabled: backup; disabled).

16 Double-click each upgraded card and verify the card loadware version in the S/W version field of the **Configuration** tab in the ITG Card Properties.

17 Use the LD 32 **ENLC** command to re-enable the Voice Gateway Media Cards.

Use LD 32 in the TTY or OTM Overlay passthru to enable the Voice Gateway Media Card with one of the following commands:

- ENLC l s c. (for Meridian 1 and Succession CSE 1000)
- ENLC c (for Option 11C or Option 11C-Mini)

18 Repeat the previous two steps for each Voice Gateway Media Card.

End of Procedure

Upgrading the Voice Gateway Media Card firmware

The minimum versions of the card firmware for the Voice Gateway Media Cards are:

- Version 6.4 for the Succession Media Card
- Version 5.6 for the ITG-P Line Card

To upgrade the card firmware, follow the steps in Procedure 29 on page 317.

Procedure 29
Upgrading the Voice Gateway Media Card firmware

1 Check the Nortel Networks Web site for the most current versions of the firmware for the ITG-P Line Card and Succession Media Card. To download firmware files from Nortel Networks, follow the steps in Procedure 111 on page 719.

2 Once the most current version of the firmware has been downloaded, follow the steps in:

- Procedure 90 on page 590 to upgrade the firmware on the ITG-P Line Card
- Procedure 91 on page 592 to upgrade the firmware on the Succession Media Card

End of Procedure

Upgrading Internet Telephone firmware

When the IP Line 3.0 loadware has been upgraded, also verify if an Internet Telephone firmware upgrade is also required. Check the *Readme First* document for the OTM IP Line 3.0 application to determine which Internet Telephone firmware version is required to be compatible. The firmware upgrade does not apply to the i2050 Soft Phone.

- In Procedure 27 on page 309, the correct loadware for the Voice Gateway Media Card should have been obtained and verified. The files should have been transferred to the OTM PC.
- If using Procedure 28 on page 314 and Procedure 30 on page 318 together, do not restart the Line card until Procedure 30 is completed. All the cards must be restarted because the software has not been upgraded. The new software will not run until the cards are rebooted, because the new firmware can be incompatible with the old software.
- If using Procedure 30 on page 318 alone (a firmware upgrade only), it is only necessary to reboot the node.

To upgrade the firmware on the Internet Telephone, follow the steps in Procedure 30. This procedure has two major steps:

- placing the Internet Telephone firmware onto each card in the node
- propagating the firmware from the card to each telephone registered on that card

Procedure 30
Upgrading the Internet Telephone firmware

1. Open OTM Navigator, and click the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.
2. Disable all Voice Gateway Media Cards for upgrading from the main card list view. All cards must have the same Internet Telephone firmware version.
3. Verify that all Voice Gateway Media Cards that require a firmware upgrade have established a signaling link with the Meridian 1 Call Server.

   Note: The Voice Gateway Media Cards must first be disabled in order to update the firmware. Use the LD 32 DISI command from OTM Maintenance Windows, the OTM system Passthru terminal, or a Meridian 1 system management terminal directly connected to a TTY port on the Meridian 1.

   To verify the link is available between the PBX and card, Telnet to each card and login. From the command line, type **pbxLinkShow**. The status of the PBX link appears. If the link is active, the screen displays the following:

   RUDPLinkState = Up
4. Select **Configuration | Synchronize | Transmit**. The **ITG - Transmit Options** dialog box is displayed.
5. Under **Transmit options**, click the **Transmit to selected nodes** radio button.
6. Under **Software download**, check the **EtherSet Firmware** check box.
7. Click on the **Browse** button to the right of the **Firmware location** text box, to locate the Internet Telephone firmware that was previously verified to be required for the Voice Gateway Media Card loadware version. Select the firmware file, and click **Open**. The path and file name of the Internet Telephone firmware appears in the **Firmware location** text box.

The IP Line 3.0 software determines the target Internet Telephone type (either i2002 or i2004) based on the firmware filename. A filename of the format xx02xxx.bin (where "x" can be any alpha-numeric character) represents a firmware file for the i2004 Internet Telephone. Similarly a filename of the format xx03xxx.bin represents a firmware file for the i2002 Internet Telephone.

CAUTION
Downloading an incorrect version of the Internet Telephone firmware can result in extended service interruptions and can require special recovery procedures.

8 Click **Start transmit** to begin upgrading the Internet Telephone firmware on the Voice Gateway Media Cards.

9 Monitor progress in the **Transmit control** window. Confirm the card firmware is transmitted successfully to all cards. Note any error messages, investigate, correct any problems, and repeat card firmware transmission until it is completed successfully on each Voice Gateway Media Card.

10 The i2004 Internet Telephones continue to run the old firmware until each telephone re-registers with a Voice Gateway Media Card that contains the new Internet Telephone firmware.

Note: Commands are available from the IPL> command line to upgrade a single i2004 Internet Telephone immediately, all i2004 Internet Telephones immediately, or schedule all i2004 Internet Telephones to be upgraded at a later time. Before doing this, verify that each card has the correct firmware version and also check the date and time on the node.

11 Select a i2004 Internet Telephone for test purposes. Telnet to the Voice Gateway Media Card. Login to the IPL> command line, and enter the following:

iSetReset "xxx.xxx.xxx.xxx"

where xxx.xxx.xxx.xxx is the IP Address of the selected telephone.

12 Monitor the display on the test telephone. As it upgrades the firmware, note the IP Address from which Voice Gateway Media Card it is receiving its upgrade.

13 Press the **Services** key (key with globe with arrow pointing East and West) on the i2004 Internet Telephone. The Services key provides access the **Telephone Options** list.

- **i.** Press **Select** to select Telephone Options.
- **ii.** Use the **Navigation** keys to scroll to **Set Info**.
- **iii.** Press the **Select** softkey, then press the **Navigation** keys until it displays **FW Version:**. For the Voice Gateway Media Card, select the appropriate firmware.

Note: For example, a firmware version can be labelled 0602B38, and this means Internet Telephone firmware version 1.38.

- 02 represents the i2004 Internet Telephone.
- B represents the Version number 1.
- 38 represents the Release number .38

14 Lift the handset and make a call to verify the telephone works.

When the telephone is working, verify the date and time on the node. Ensure each card has the correct loadware and firmware before using the umsUpgradeAll command to upgrade all the telephones.

15 To verify the date and time on the node from OTM, select the node in the top of the **IP Telephony Gateway - IP Line 3.0** window.

Double-click on Leader 0 in the bottom of the window. The **ITG Card Properties** window appears.

Note: Cards receive their time from the Leader card. If the time for Leader 0 is correct, all cards on the node should be the same. If Leader 0 displays the incorrect time, reset the time. The time propagates to the other cards.

16 Click the **Maintenance** tab. This displays the **Node time**. If the time is incorrect, click on the **Set Node Time** button. The Set Node Time window opens. Under **Time and date**, set the **Time**, where the time is displayed in the HH:MM:SS AM/PM format. Click **OK** to close the window.

17 Click the **Configuration** tab. Note the card's loadware version (**S/W version**) and the Internet Telephone firmware version (**i2002** or **i2204 F/W version**).

Double-click on each card to verify the loadware and firmware version. This must be done for every card.

18 Before proceeding, ensure the time of the card is set correctly. Telnet to each Voice Gateway Media Card and login. At the IPL> command line, enter the following:

umsUpgradeAll "hh:mma/p"

hh:mma/p specifies the time when the upgrade will occur, **a** represents A.M., and **p** represents P.M. The time is in Standard format.

For example, umsUpgradeAll “11:30a” or umsUpgradeAll “2:45p”.

At the time specified, all the i2004 Internet Telephones on the Voice Gateway Media Card go out of service. This can take several minutes.

Upon completion of the firmware upgrade, the i2004 Internet Telephones are brought back online in groups of ten.

CAUTION

The umsUpgradeAll command (without the time parameter) causes the i2004 Internet Telephones registered on all cards you are logged into to be immediately taken out of service, unless the time parameter is specified.

After the test telephone is working, the umsUpgradeAll does not need the time parameter. However, without the time parameter, the command immediately resets all the i2004 Internet Telephones currently registered on that line card.

If the technician does not want to immediately reset all the phones, and wants to schedule the reset time of the i2004 Internet Telephones, check the time on all the cards. If necessary, reset the time to ensure all cards have the same time. Then issue the umsUpgradeAll "hh:mma/p" command, where "hh:mma/p" represents the time when the upgrade will occur.

19 At the IPL> prompt, verify the i2004 Internet Telephone are upgraded for each Voice Gateway Media Card by entering the following:

isetShow

Inspect the list to ensure all i2004 telephones have the correct firmware version.

20 For any i2004 Internet Telephones that did not upgrade successfully, try one of the following (in order):

- use the **isetReset "IP Address"** command
- enter the following combination of keystrokes at the telephone console: **release**, **mute**, **up**, **down**, **up**, **down**, **up**, **mute**, **9**, **release**
- power the telephone off and then on again

If the upgrade was unsuccessful on any of the i2004 Internet Telephones, this is most likely due to one of the following reasons:

- one of the Voice Gateway Media Cards did not upgrade the software successfully
- an i2004 Internet Telephone is loaded with a firmware version that was unable to be upgraded by the Voice Gateway Media Card in the normal way
- the umsUpgradeAll command was not issued
- one of the cards has not been reset

If the upgrade was unsuccessful, re-do the appropriate procedure. If the upgrade is still unsuccessful, contact your technical support representative for further assistance.

End of Procedure

For additional information on configuring the i2004 Internet Telephone and the i2050 Software Phone, see *Internet Terminal: Description Guide* (553-3001-217).

Configuring OTM Alarm Management to receive IP Line SNMP traps

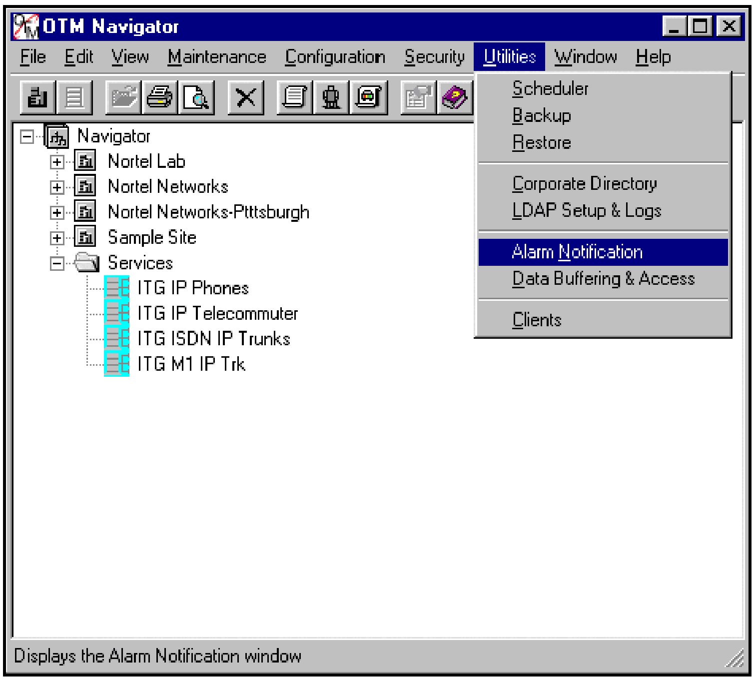
To configure the alarm notification feature in OTM to receive SNMP traps, follow the steps in Procedure 31.

For more information about OTM Alarm Management, refer to *Using Optivity Telephony Manager 2.0* (553-3001-330).

Procedure 31
Configuring SNMP Traps

1 In the **OTM Navigator** window, select the **Utilities** menu option and then click on **Alarm Notification** (see Figure 51).

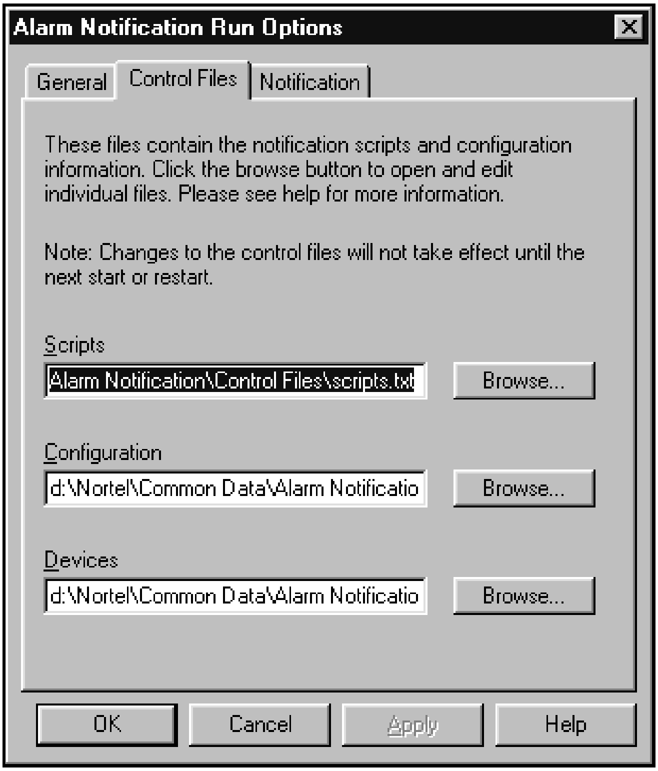
Figure 51
OTM Navigator–Utilities | Alarm Notification



2 The **OTM Alarm Notification** window opens. Select **Configuration | Run Options**.

3 The **Alarm Notification Run Options** dialog box opens. Click the **Control Files** tab (see Figure 52).

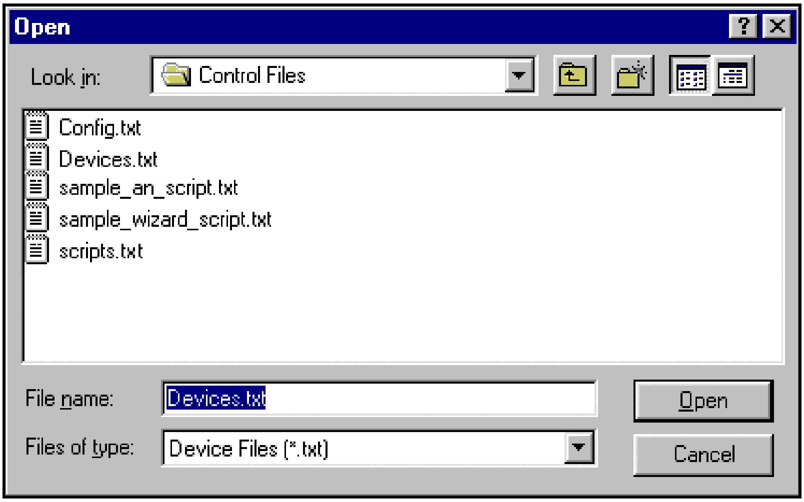
Figure 52
Alarm Notification Run Options–Control Files tab



4 Click the **Browse** button located to the right of the **Devices** text box. The **Open** dialog box opens.

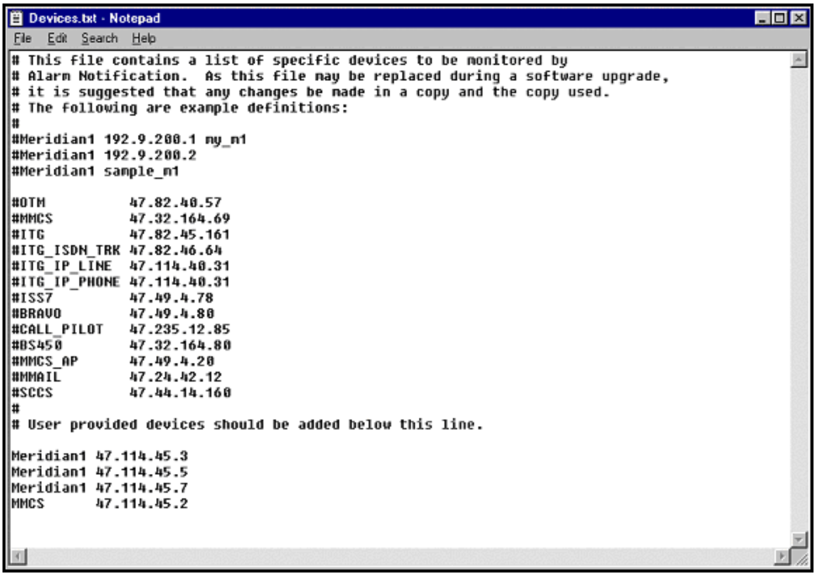
5 Select the **Devices** file from the Control Files folder and click **Open** (see Figure 53 on page 325).

Figure 53
Open dialog box



6 The Devices.txt file opens (see Figure 54 on page 326).

Figure 54
Devices.txt file




```
# This file contains a list of specific devices to be monitored by
# Alarm Notification.  As this file may be replaced during a software upgrade,
# it is suggested that any changes be made in a copy and the copy used.
# The following are example definitions:
#
#Meridian1 192.9.200.1 my_m1
#Meridian1 192.9.200.2
#Meridian1 sample_m1

#OTM           47.82.40.57
#MMCS          47.32.164.69
#ITG           47.82.45.161
#ITG_ISDN_TRK 47.82.46.64
#ITG_IP_LINE  47.114.40.31
#ITG_IP_PHONE 47.114.40.31
#ISS7          47.49.4.78
#BRAVO         47.49.4.80
#CALL_PILOT    47.235.12.85
#BS450         47.32.164.80
#MMCS_AP       47.49.4.20
#MMAIL         47.24.42.12
#SCCS          47.44.14.160
#
# User provided devices should be added below this line.

Meridian1 47.114.45.3
Meridian1 47.114.45.5
Meridian1 47.114.45.7
MMCS      47.114.45.2
```

7 For each Voice Gateway Media Card in each monitored IP Telephony node, add a line consisting of three fields separated by spaces, as shown in Table 63 on page 327. Enter the first line under the last line that begins with a "#".

8 Click **File | Save As**. Save the template to a new file, for example, **ITGDevices1.txt**, to avoid overwriting the template file.

9 In the **Alarm Notification Run Options** window, verify that the devices field name is correct (ITGDevices1.txt). Click **Apply**, and then **OK**.

Note: OTM Alarm Notification must be restarted whenever Control Files are changed.

10 If OTM Alarm Notification is running (the red traffic light is showing on the toolbar), click on the red traffic light to stop alarm notification. The traffic light changes to green. Click the green traffic light to restart alarm notification. The traffic light should turn to red to indicate it is running.

If OTM Alarm Notification is not running, as indicated by the green traffic light, click on the green traffic light to change it to red. This starts Alarm Notification.

11 Telnet to each Line card, login and at the IPL> command line, enter the **itgAlarmTest** command. A series of SNMP traps is emitted by the Voice Gateway Media Card and appears in the OTM Alarm Notification browser window. Verify the device name identifies the correct Voice Gateway Media Card.

Table 63
Format of Devices.txt file

Device Type	IP Address	Device Name
ITG_IP_PHONE	xxx.xxx.xxx.xxx	Site_Leader_0
ITG_IP_PHONE	xxx.xxx.xxx.xxx	Site_Leader_1
ITG_IP_PHONE	xxx.xxx.xxx.xxx	Site_Follower_2

For every Voice Gateway Media Card in every node, there is a line in the table. For example, a line in the table can look like this:

ITG_IP_PHONE 192.9.200.1 MySite_MySystem_Leader_1

The following is a description of each field in the table:

Device Type – is a dedicated receive string or name used as an index for the IP Line application. The Device Type must be ITG_IP_PHONE.

IP Address – the source IP address on the Voice Gateway Media Card from which the traps are coming (either the card Voice IP address (TLAN) or card Management IP address (ELAN)). By default, the SMNP traps are issued from the card Voice IP address (TLAN). If you have previously configured a card routing table entry on the IP Telephony node pointing to the IP address of the OTM, then the SMNP trap issues from the Management IP address (ELAN) of the card.

Device Name – the device name can be any string. Nortel Networks recommends that abbreviations for the site and system, the card functions, and the terminal numbers (TNs) are used, such as Site_System_Leader/Follower_TN. Note: Spaces should not be used in the Device Name. Use an underscore (_) as a separator.

The Leader card has two IP addresses, the card voice IP address and the node IP address. The Follower cards have only a single IP address, the card voice IP address.

End of Procedure

Assemble and install an Internet Telephone

To assemble and install an Internet Telephone, refer to the *Internet Terminals Description* (553-3001-217).

Change the default IPL> CLI Shell password

The IPL> Command Line Interface (CLI) is password protected for Telnet access and access to the local maintenance port. The same user name and password also protects FTP access to the Voice Gateway Media Card. The IPL> CLI has a default user name of itgadmin and a default password of itgadmin.

The default user name and password must be changed as a preventative security measure. See “Changing the IPL> CLI Shell user name and password” on page 411 and Procedure 55 on page 415.

Configure the Internet Telephone Installer Passwords

The Internet Telephone Installer Password protection, for changing the TN on the telephone, controls registration with a virtual line TN on the Call Server. See page 420 for more information about the Internet Telephone Install Passwords.

To enable and set the administrative Internet Telephone Installer Password, see Procedure 58 on page 429. If needed, enable and set a temporary Internet Telephone Installer Password. See Procedure 59 on page 433.

Configuration of IP Telephony Nodes using Element Management

Contents

This section contains information on the following topics:

Reference list

The following are references for this section:

- *Internet Terminals Description* (553-3001-217)
- *Element Management* (553-3023-222)

Overview

This chapter explains how to configure IP Telephony nodes and Voice Gateway Media Cards using Element Management. Element Management is accessed using a PC with a Web browser. The PC must be connected to a LAN that has access to the Signaling Server's Node IP address, either directly or routed through the network.

> ***Note:*** The ELAN IP address may be required, instead of the Node IP address, to access to the Element Management login page in secure environments.

This chapter also provides instruction for transmitting files to Voice Gateway Media Cards; upgrading card loadware; and upgrading i2002/i2004 Internet Telephone firmware.

Read the "IP Network Engineering Guidelines" on page 133 before installing an IP Telephony node.

Upgrading the ITG-P Line Cards to IP Line 3.0

Succession CSE 1000 Rel 2.0 requires the ITG-P Line Cards to be running IP Line 3.0. Element Management cannot be used with the ITG-P Line cards running any IP Line application prior to IP Line 3.0.

WARNING

The ITG-P Line Card with earlier release of the IP Line application must be upgraded to IP Line 3.0 or communication with Element Management fails.

OTM 2.0 is required to upgrade an ITG-P Line Card to IP Line 3.0. Once the card's loadware has been upgraded to IP Line 3.0 using OTM, configuration, administration, and maintenance tasks can be performed using Element Management.

Refer to "ITG-P card upgrades" in the *Upgrades* (553-3023-258) for the procedure to upgrade an ITG-P Line card to IP Line 3.0 loadware.

Configure IP Line data using Element Management

Element Management can be used to manually add and configure an IP Telephony node on Succession CSE 1000 Release 2.0 systems. Multiple nodes can be configured and managed from Element Management.

A node is defined as a collection of Signaling Servers and Voice Gateway Media Cards. Each node in the network has a unique Node ID. This Node ID is an integer value. A node has only one primary Signaling Server or Leader Voice Gateway Media Card. All the other Voice Gateway Media Cards are defined as Followers.

Note 1: All IP addresses and subnet mask data must be in dotted decimal format. Convert subnet mask data from Classless Inter-Domain (CIDR) format.

Note 2: See Table 45 on page 209 and for IP addresses and information required in this procedure.

Note 3: The following sections discuss how to configure IP Line using Element Management. The following three sections (of the IP Telephony section) in Element Management are not covered in this NTP:

- SNTP (see *IP Peer Networking* (553-3023-220)
- Gatekeeper (see *IP Peer Networking* (553-3023-220)
- Signaling Server (see *Installation and Configuration* (553-3023-210)

Internet Explorer browser configuration

Succession CSE 1000 Element Management requires Microsoft Internet Explorer 5.5 or 6.0. Element Management is not supported on the Netscape browser. The PC should be PIII with a 500 MHz processor (at minimum).

Internet Explorer caching interferes with the Element Management application, in that users cannot see real-time changes as they occur. For this reason, Internet Explorer caching must be turned off.

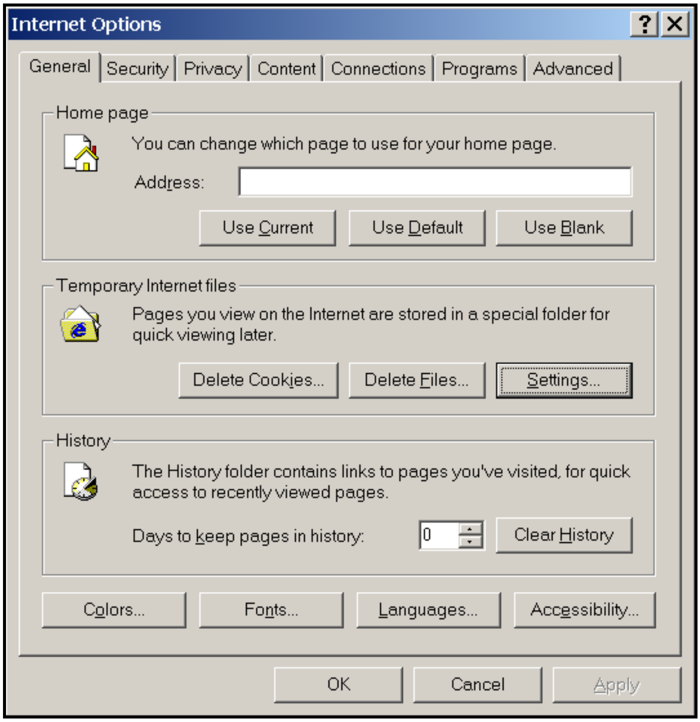
Follow the steps outlined in Procedure 32 on page 333 to prevent caching of Web pages by the Internet Explorer browser.

Procedure 32
Turning off browser caching in Internet Explorer

1 Launch Internet Explorer.

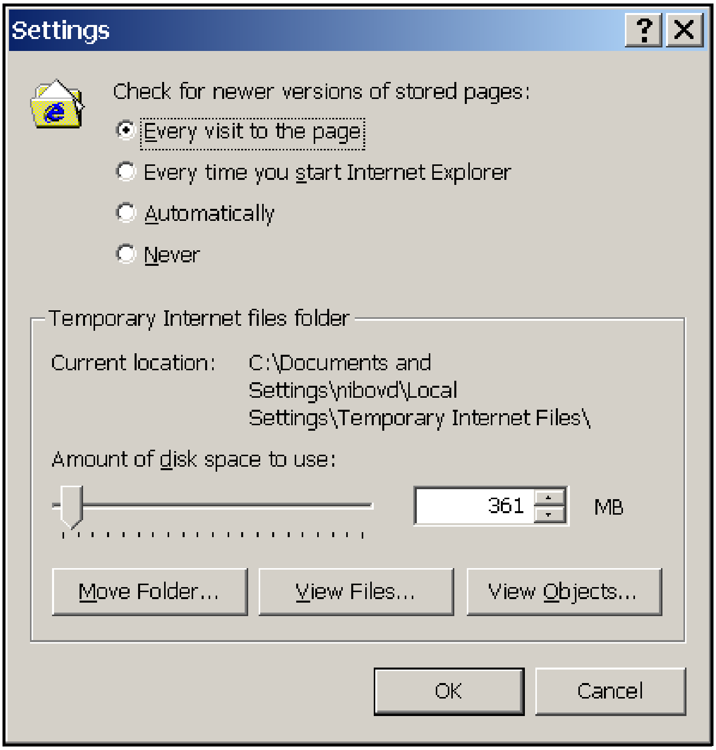
2 Click **Tools | Internet Options**. The Internet Options window opens (see Figure 55 on page 333).

Figure 55
Internet Explorer - Internet Options



3 On the **General** tab, under the **Temporary Internet files** section, click the **Settings** button. The Settings window opens (see Figure 56 on page 334).

Figure 56
Temporary Internet files Settings window



4 Click the **Every visit to the page** radio button. This checks for new versions of stored pages on every visit to the Web page.

5 Click **OK** in the Settings window.

6 Click **OK** in the Internet Options window.

End of Procedure

Launching Element Management

Procedure 33
Launching Element Management

1 Open a Web browser.

2 Enter the **Signaling Server Node IP address** in the Address Bar of the browser window and press **Enter** on the keyboard.

Note: The ELAN IP address may be required, instead of the Node IP address, to access to the Element Management login page in secure environments.

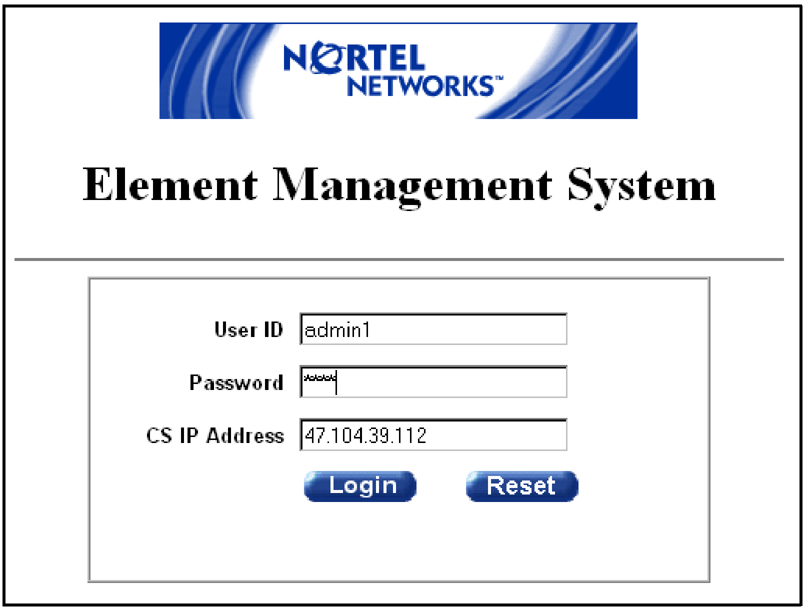
3 The Element Management opens and the **Login** page appears (see Figure 57).

a. Enter the **User ID** and **Password** of the Call Server.

b. Enter the IP Address of the Call Server in the **CS IP Address** field.

c. Click the **Login** button.

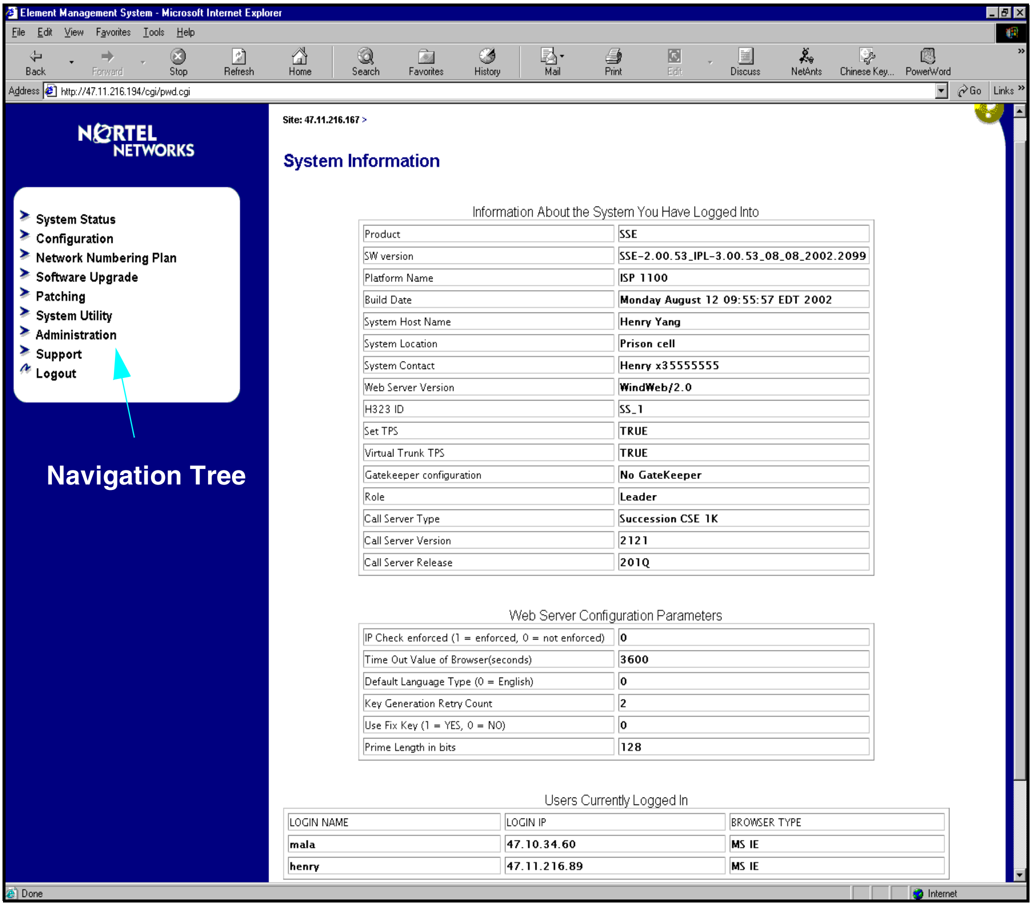
Figure 57
Element Management–Login page



4 The **System Information** page appears (see Figure 58).

The **Navigation Tree** is located on the left side of the browser window. The **System Status** menu is expanded in Navigation Tree.

Figure 58
Element Management–System Information



Note 1: To log out of Element Management, click **Logout** at the bottom of the Navigation Tree.

Note 2: When a user is on the Configuration -> IP Telephony -> Edit page, Element Management times out after a period of inactivity (see Figure 61 on page 341). Users are prompted with a warning five minutes before Element Management times out. If the user clicks OK within the warning time out period, the timer is reset. If the user does not respond, the session is cancelled and the user is forced to login again. Any data that was modified, but not submitted, is lost.

End of Procedure

Summary of Procedures

The following is the summary of steps required to configure a node and a Voice Gateway Media Card using Element Management:

1 "Manually adding an IP Telephony node" on page 338

2 "Configuring SNMP traps and community name access for security" on page 343

3 "Configuring DSP Profile data" on page 346

4 "Configuring Quality of Service (QoS)" on page 351

5 "Configuring the ELAN IP address (Active ELNK), TLAN voice port, and Routes" on page 353

6 "Configuring File Server access" on page 358

7 "Configuring Loss and Level Plan" on page 360

8 "Configuring the card properties of the Voice Gateway Media Card" on page 361

9 "Submitting and transferring the node information" on page 364

Manually adding an IP Telephony node

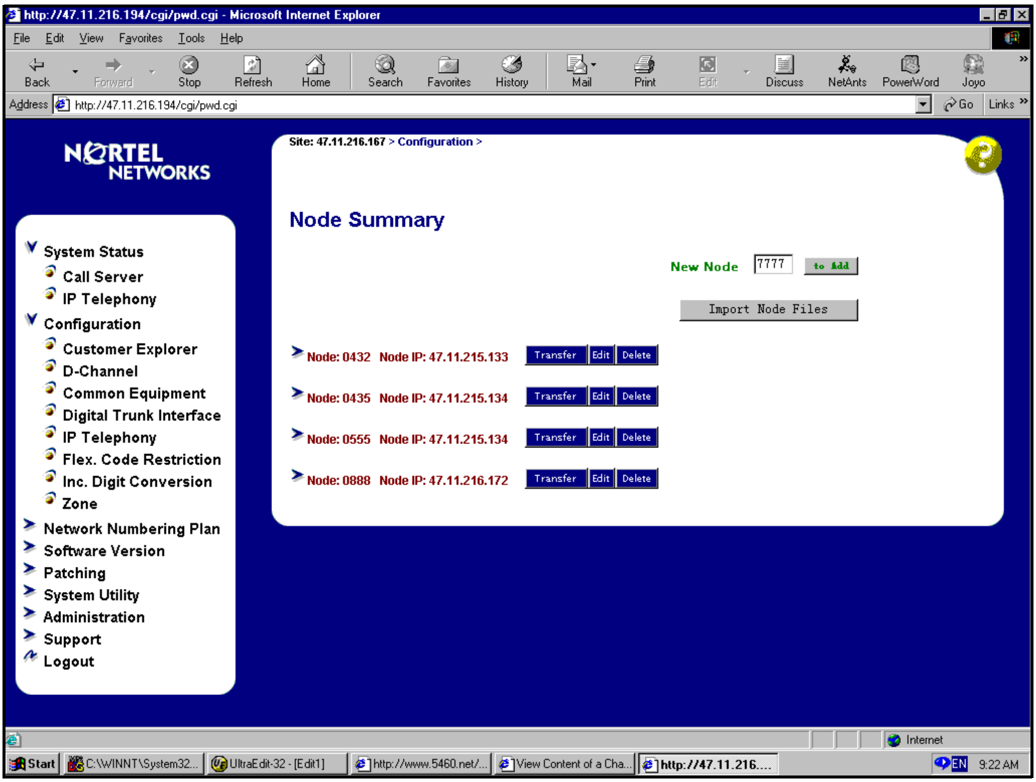
Follow the steps in the following procedure to add an IP Telephony node using Element Management.

Procedure 34
Adding an IP Telephony node manually

1 To manually add a new IP Telephony node, click **Configuration** in the Navigation Tree.

2 In the Configuration menu, click **IP Telephony**. The **Node Summary** page appears (see Figure 59).

Figure 59
Element Management–Node Summary–Adding a new node



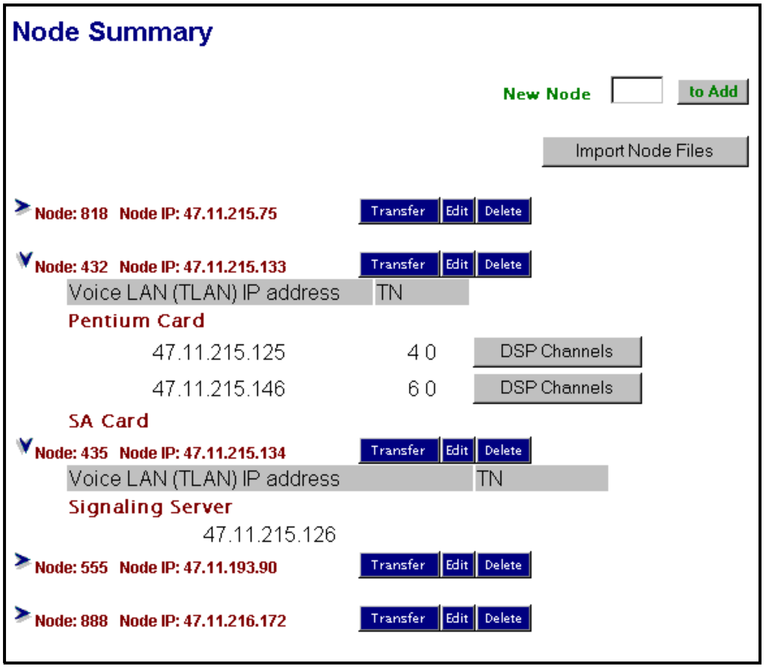
If this is the first node to be added, the “No nodes are configured” message is displayed. The technician has the option to either “Add a New Node” or “Import Node Files”.

The Node Summary pages shows a list of all the configured nodes. To expand a node and view its elements, click the arrow (>) to the left of the Node information. Figure 60 on page 340 shows two expanded nodes.

There are five buttons on the Node Summary page:

- **to Add** - This button is used to add a new IP Telephony node. Enter an unused Node ID and then click to Add.
- **Import Node Files** - This button imports the configuration files from an existing node.
- **Transfer** - This button transmits/transfers changes to the selected IP Telephony node.
- **Edit** - This button opens an Edit properties page for the selected IP Telephony node.
- **Delete** - This button deletes the selected IP Telephony node.

Figure 60
Node Summary - expand a node



3 Enter the new Node ID in the **New Node** text box. The Node ID is one to four digits in length.

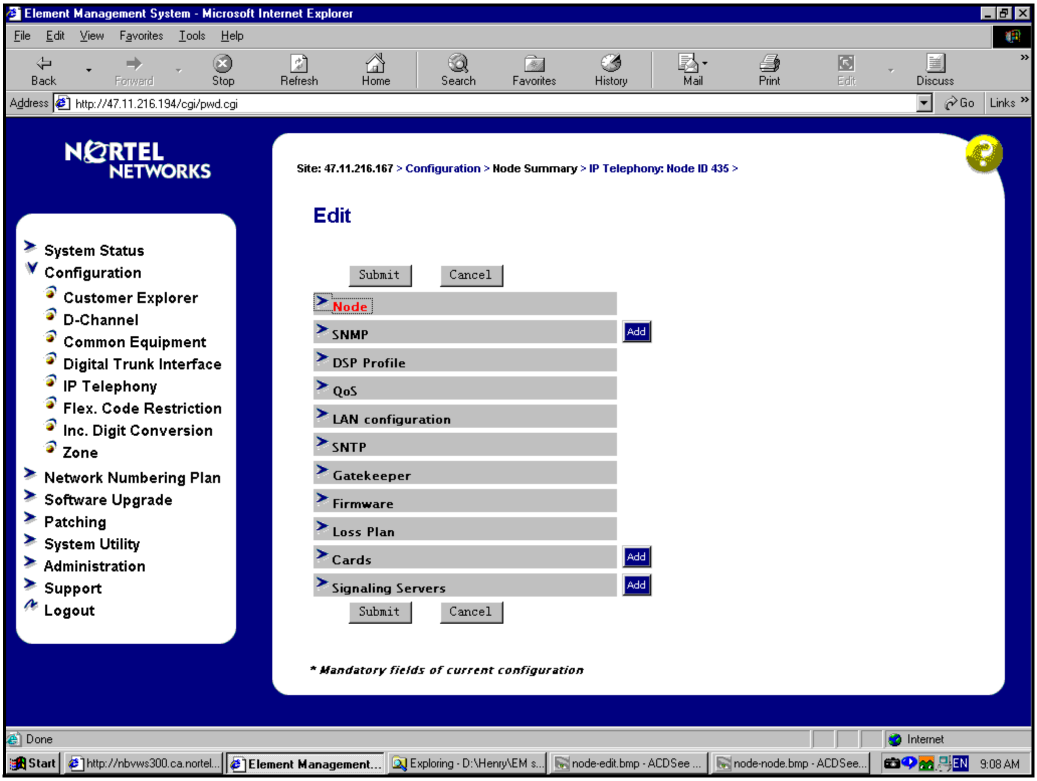
CAUTION

The Voice Gateway Media Cards identify themselves with a node using the node number or node ID. If there are multiple IP Telephony nodes sharing the same TLAN, each node must have a unique ID. Each system on the TLAN must have a unique node ID assigned to the Voice Gateway Media Cards on the system.

Note: The Node ID field corresponds to the Node ID field in the Internet Telephone configuration. Write down the node number, which is used during the Internet Telephone configuration.

4 Click the **to Add** button. The **Edit** page opens (see Figure 61).

Figure 61
Element Management–Edit

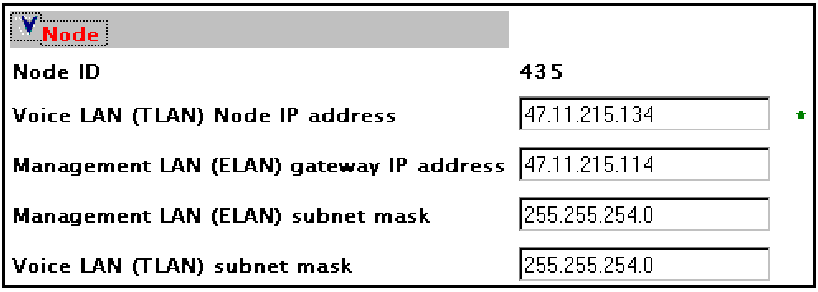


There are three buttons on the Edit page:

- **Submit** - This button transmits changes to the Call Server and returns the users to the Node Summary page.
- **Cancel** - This button discards changes made to the IP Telephony node and returns the users to the Node Summary page.
- **Add** - The Add buttons are associated with specific sections of the IP Telephony node properties. The user can add a new SNMP trap, Cards, and Signaling Servers.

5 Click **Node** to edit the Node information, if it is not already expanded by default (see Figure 62 on page 342).

Figure 62
Configuration > Node Summary > Edit > Node



a. **Node ID:** The node ID entered on the previous page appears.

b. **Voice LAN (TLAN) Node IP address:** Enter Voice LAN (TLAN) Node IP address in dotted decimal format. The Voice LAN Node IP is on the TLAN. The Node IP address is the IP address used by the Internet Telephones to communicate with the Voice Gateway Media Cards on the TLAN. If a Voice Gateway Media Card becomes the primary (Leader) during an election, it assigns itself the Node IP address.

Note: A green asterisk (*) indicates that a field is a required / mandatory field.

c. **Management LAN (ELAN) gateway IP address:** Enter Management LAN (ELAN) gateway IP address in dotted decimal format. This is the IP address of the gateway of the subnet to which the Voice Gateway Media Card belongs. This is the IP address of the router interface on the ELAN, if present. If there is no management LAN gateway, enter 0.0.0.0.

d. **Management LAN (ELAN) subnet mask:** Enter Management LAN subnet mask address in dotted decimal format. This is the subnet mask that is used along with the ELAN IP address to identify which subnet the Voice Gateway Media Card belongs.

e. **Voice LAN (TLAN) subnet mask:** Enter Voice LAN subnet mask address in dotted decimal format. This is the subnet mask that is used along with the TLAN IP address, to identify the subnet to which the Voice Gateway Media Card belongs.

Note: Do not click Submit until all the node information has been entered. If the Submit button is clicked prematurely, the Node Summary page reappears. To continue the configuration, click the Edit button to return to the Node Edit page.

End of Procedure

Configuring SNMP traps and community name access for security

Procedure 35 explains how to change the SNMP community names and to set SNMP traps.

The SNMP community names provide better security for the IP Telephony node. Element Management uses the community name password to refresh the Voice Gateway Media Card status, and to control the transmitting and retrieving of configuration data files for database synchronization.

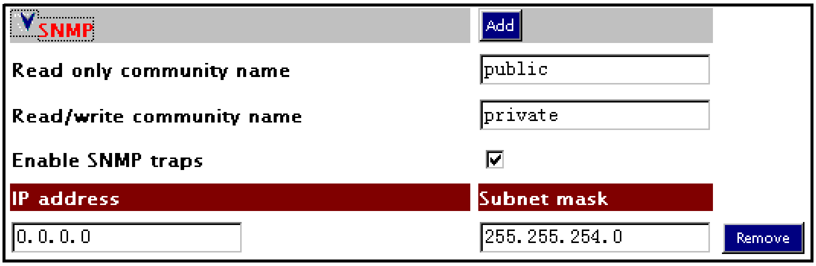
Note: If the community names are forgotten, connect a TTY to the Voice Gateway Media Card maintenance port. Restart the card. The card displays the community name on the TTY during startup.

To configure the SNMP traps and community names, follow the steps in Procedure 35 on page 344.

Procedure 35
Configuring SNMP

1 Click **SNMP** (see Figure 63 on page 344).

Figure 63
Configuration > Node Summary > Edit > SNMP



- **a.** **Read only community name:** Leave the default selection.
- **b.** **Read/write community name:** Leave the default selection.
- **c.** **Enable SNMP traps:** Check the Enable SNMP traps checkbox, if configuring one or more SNMP management IP addresses to receive SNMP traps from cards in the IP Telephony node.
- **d.** **IP address:** If SNMP traps are enabled, the SNMP traps are sent to the IP address entered here.
- **e.** **Subnet mask:** If SNMP traps are enabled, this is the subnet mask of where SNMP traps are sent.

  IP addresses that are added here create special card routing tables that direct packets out the ELAN and ELAN gateway. Exercise caution when adding entries since the entry could result in one-way voice transmission if a change results in voice packets being streamed out the ELAN instead of the TLAN interface.

To add an SNMP Manager IP address, click the **Add** button, and then type the IP address in the SNMP traps entry fields. Add SNMP Manager IP addresses for:

- the local or remote OTM server
- PPP IP address configured in the Netgear RM356 Modem Router, or equivalent, on the ELAN for the remote support OTM PC
- the SNMP manager for remote alarm monitoring

Note 1: Up to eight SNMP trap servers can be defined.

Note 2: A net route or host route through the management gateway is added to the Voice Gateway Media Cards IP Routing Table for each SNMP management address that is added to the SNMP traps list.

Note 3: Element Management does not provide an SNMP alarm browser. If SNMP alarm collection is required, the OTM Alarm Manager is recommended.

Note 4: To remove and SNMP trap server, click the corresponding **Remove** button.

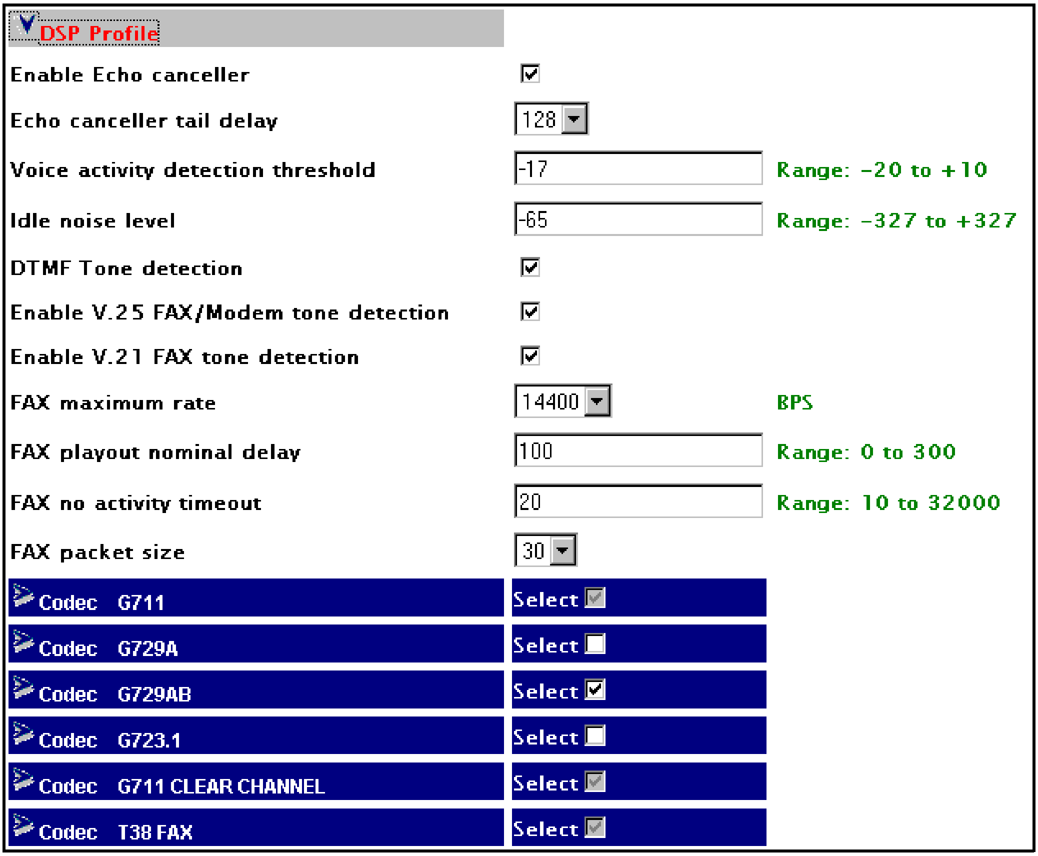
End of Procedure

Configuring DSP Profile data

Procedure 36
Configuring DSP Profile data

1 Click **DSP Profile**. The DSP Profile page opens (Figure 64). The DSP Profile area includes DSP Profile information and a list of codecs.

Figure 64
Configuration > Node Summary > Edit > DSP Profile



2 Under **DSP Profile** leave the values at their default settings unless directed to change them by Nortel Networks Field Support.

a. **Enable Echo canceller:** The echo canceller is enabled by default. Do not uncheck this box. Never disable echo canceller unless directed by Nortel Networks Field Support.

b. **Echo canceller tail delay:** Select the maximum value available. The default value is 128ms. Never reduce the echo canceller value unless otherwise directed by Nortel Networks Field Support.

c. **Voice activity detection threshold:** The default value is -17db. The range is -20db to +10db.

d. **Idle noise level:** The default value is -65db. The range is -327db to +327db.

e. **DTMF Tone detection:** Ensure this is checked to enable DTMF tone detection. This is enabled by default.

f. **Enable V.25 FAX/Modem tone detection:** Ensure this is checked to enable V.25 FAX/Modem tone detection. This is enabled by default.

g. **Enable V.21 FAX tone detection:** Ensure this is checked to enable V.21 FAX tone detection. This is enabled by default.

h. **FAX maximum rate:** The FAX maximum rate is one of the following values: 2400, 4800, 7200, 9600, 12000, or 14400. The default value is 14400 bps.

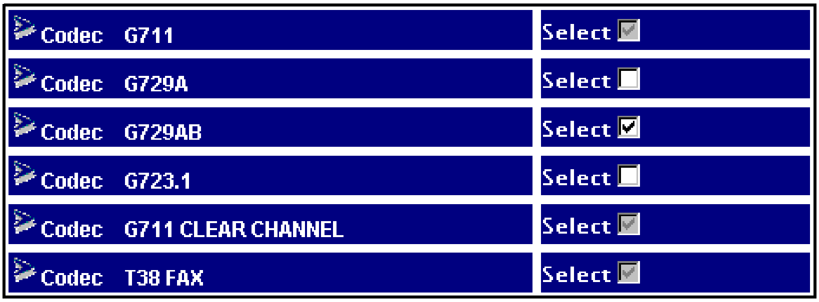
i. **FAX playout nominal delay:** The default value is 100ms. The range is 0ms to 300ms.

j. **FAX no activity timeout:** The default value is 20secs. The range is 10secs to 32000secs.

k. **FAX packet size:** Select the packet size. The default value is 30 bytes. The range is 20-48 bytes.

3 To select a codec, scroll through the list, and click the corresponding **Select** check box (see Figure 65 on page 348 for codecs samples).

Figure 65
Codec list



Note: The Codec list contains six codec settings for G.711, G.729A, G.729AB, C.723.1, G711 Clear Channel, and T38 FAX for the Voice Gateway Media Card.

4 The G.711, G711 Clear Channel, and T38 FAX codecs are selected by default and these selections cannot be cleared. However:

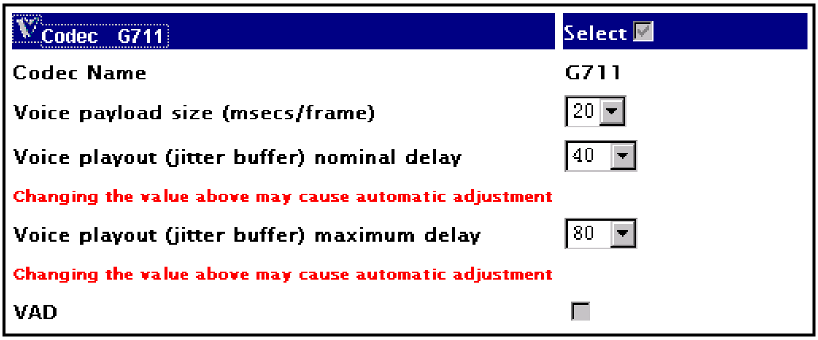
- The payload size, jitter buffer setting, and companding law for the G.711 codec can be changed.
- Only the jitter buffer can be changed for the G.711 Clear Channel codec.

  Up to three additional codecs can be optionally selected. The user can select the G.729A, G.729AB, and/or G.723.1 codecs.
- If the G.729A or G.729AB codec are selected, the user can change the payload and jitter buffer.
- If the G.723.1 codec is selected, only the jitter buffer can be changed. The payload size of 30 msec is the only supported payload.

Note: The G.723.1 codec is supported only on Succession CSE 1000 Release 2.0 systems. The supported G.723.1 codec has bit rates of 5.3 Kbps and 6.3 Kbps.

5 Expand the selected **Codec** (Figure 66 on page 349):

Figure 66
Selected codec



Element Management performs some jitter buffer adjustments on the browser side. The following describes the jitter buffer adjustment that are made in Element Management:

- A change of payload resets the Nominal Voice Playout (NVP) and Maximum Voice Playout (MVP) values to the default recommended values:

  NVP = 2 * payload
  MVP = NVP + 2 * payload

- A change of NVP value changes the MVP value to the default (MVP = NVP + 2 * payload) and changes the values listed in the MVP pull down list so the minimum value listed does not violate the requirement of NVP + 2 * payload.

- The MVP value can be changed by the user. The pulldown values range from the minimum recommended value (see above) up to the maximum allowed value for the selected codec type.

6 Set the following values for the codec:

a. Codec Name: The codec name is based on the selected codec.

b. Voice payload size (msecs/frame): The payload size is determined by the selected codec.

For each codec type, the payload is defaulted to the maximum supported: 30 msec for G.711 (a-law and mu-law), 50 msec for G.729A, 50 msec for G.729AB, and 30 msec for the G.723.1.

Note: If there are multiple nodes on a system and the same codec is selected on more than one node, ensure that each node has the same voice payload size configured for the codec.

c. Voice playout (jitter buffer) nominal delay: Set the nominal value to highest setting that the device allows. The range is 20 to 200ms and is dependent by the codec. Changing this value, can cause the automatic adjustment of the other settings for this codec. For more information, see “Adjusting jitter buffer size” on page 189.”

d. Voice playout (jitter buffer) maximum delay: The maximum delay has a range of 60 to 500ms and is dependent on the codec. Changing this value, can cause the automatic adjustment of the other settings for this codec.

e. VAD: Check the VAD check box to enable voice activity detection.

7 Repeat the last step for each of the selected codecs.

End of Procedure

Configuring Quality of Service (QoS)

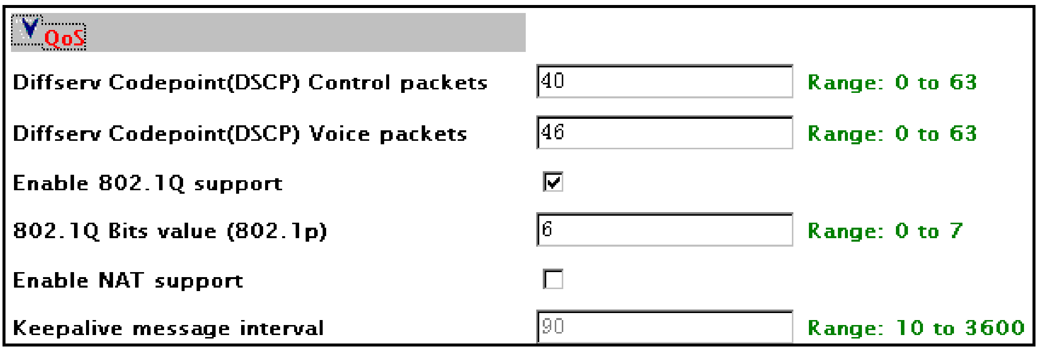
The QoS section includes the settings for:

- DiffServ Codepoint (DSCP)
- 802.1Q support
- NAT support

Procedure 37
Configuring QoS

1 Click **QoS** (see Figure 67).

Figure 67
Configuration > Node Summary > Edit > Qos



2 The Differentiated Service (DiffServ) Codepoint (DSCP) determines the priorities of the management and voice packets in the IP Line network. The range for both management and voice packet DiffServ is 0-63 inclusive.

The DiffServ value can be configured, if required, to obtain better QoS over the IP data network (LAN/WAN).

The value entered depends on the policy in the customer's data network.

Note: Do not change DiffServ from the default values unless instructed by the IP network administrator.

Under **QoS**, modify the Control priority and Voice priority values only as directed by the IP network administrator.

The recommended configuration values are:

a. **Diffserv Codepoint (DSCP) Control packets:** A value of 40 - Class Selectore 5 (CS5). The range is 0-63. This sets the priority of the signaling messaging.

b. **Diffserv Codepoint (DSCP) Voice packets:** A value of 46 Control DSCP - Expedited Forwarding (EF). The range is 0-63.

3 802.1Q enables Virtual LANs (VLANs) to be defined within a single LAN. This improves bandwidth management and limits the impact of broadcast and multicast messages.

a. **Enable 802.1Q support:** 802.1Q support is disabled by default.

b. **802.1Q Bits value (802.1p):** The priority field is a 3-bit value, with a default value of 6. The range is 0-7. A value of 6 is recommended by Nortel Networks. The p bits within the 802.1Q standard enables packet prioritization at Layer 2 improving network throughput for IP Telephony data.

4 NAT provides mapping of public to private addressing. Support for networks containing NAT devices has been enhanced with the addition of a periodic message that is sent to prevent the RTP packet stream's NAT session from timing out. This could occur when the Internet Telephone is muted or on hold, and packet transmission is stopped.

a. **Enable NAT support:** Click this check box to enable the periodic sending of the session Keep Alive message. By default, this is disabled and the message is not sent.

b. **Keepalive message interval:** The field defines the delay between transmissions of the dummy message. The default value is 90 seconds. The range is 10–3600 seconds. Set this value to a value that is shorter than the NAT device's session timeout value.

End of Procedure

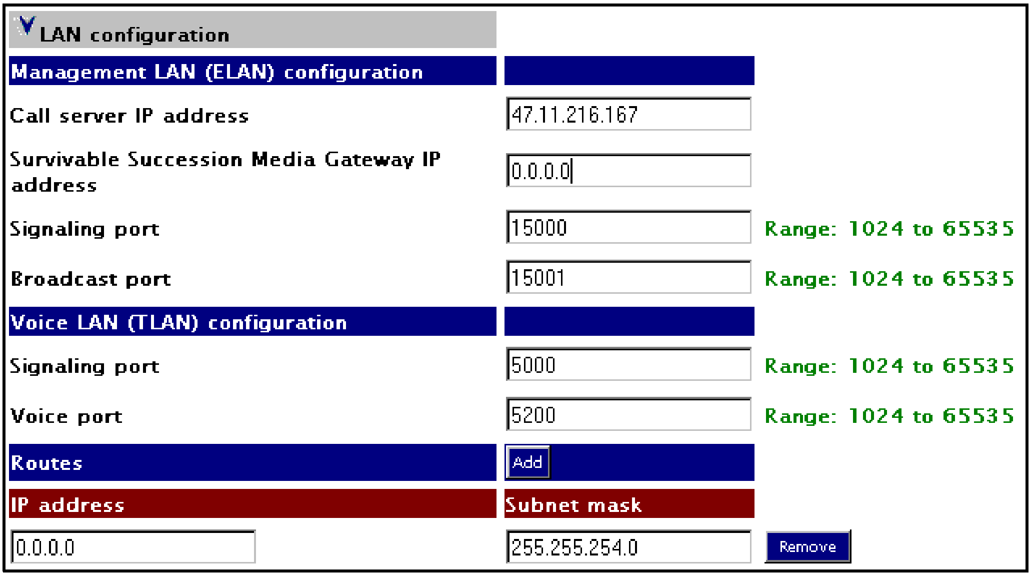
Configuring the ELAN IP address (Active ELNK), TLAN voice port, and Routes

The LAN configuration section is used for configuring the Call Server ELAN IP address (Active ELNK), TLAN Voice port, and Routes.

Procedure 38
Configuring the Call Server ELAN IP address (Active ELNK), TLAN voice port, and Routes

1 Click **LAN Configuration** (see Figure 68)

Figure 68
Configuration > Node Summary > Edit > LAN configuration



2 Enter the following **Management LAN (ELAN) configuration** settings:

a. Call Server IP address: This is the IP address of the Call Server on the Embedded LAN (ELAN). Enter the Call Server ELAN IP Address (Active ELNK).

Note: The Call Server ELAN IP address must correspond to the Active ELNK IP address configured in LD 117. It must be in the same subnet as the ELAN for the IP Line node.

b. Survivable Succession Media Gateway IP address: This address is configured for survivability. It is the IP address of the Survivable Succession Media Gateway on the ELAN.

Note 1: The Survivable Succession Media Gateway IP address must correspond to the Active ELNK IP address. If configured, all Voice Gateway Media Cards in the same node should be in the same Survivable Cabinet.

Note 2: The Survivable Media Gateway associated with the primary Signaling Server IP Telephony node is called the Alternate Call Server. It is normally located in the same equipment rack with the Call Server and Signaling Server, therefore it is normally connected to the same ELAN subnet as the Call Server and the primary Signaling Server IP Telephony node. The Alternate Call Server Media Gateway is equipped with sufficient trunk cards, Voice Gateway Media Cards, and centralized Call Pilot, so that it provides a large degree of survivability in case of Call Server equipment failure for Internet Telephone users who normally register through the Signaling Server.

Refer to *Planning and Engineering Guidelines* (553-3023-102) and *Installation and Configuration* (553-3023-210) for more information about survivability.

c. Signaling port: The default value is 15000. The range is 1024 to 65535.

d. Broadcast port: The default value is 15001. The range is 1024 to 65535.

3 Under **Voice LAN (TLAN) configuration**:

a. **Signaling port:** The default value is 5000. The range is 1024 to 65535. The TLAN Signaling occurs on UDP ports 7300, 4100, 5100, and 5000.

b. **Voice port:** Change the Voice port only as instructed by the IP network administrator to improve Quality of Service for the Internet Telephones. For example, if RTP Header compression is used to reduce voice bandwidth on narrow band WAN links, then TLAN voice port range needs to be set to 16384 or higher. The exact range is provided by the system administrator. The TLAN Voice port range is 1024 to 65535. The default Voice ports are 5200 - 5295.

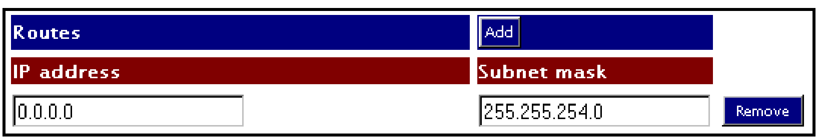
CAUTION

Do not set the Voice port to a value that is already used for signaling (4100, 5000, 5100, 7300).

The Voice port defines the first port in a range spanning the gateway channels on the card; this means a Voice port value of 5200 reserves ports 5200-5263 on the Succession Media Card and 5200-5247 on the ITG-P Line Card. If this value is changed from the default, confirm the selected Voice port value does not range into one of the reserved signaling port values.

4 Click the **Add** button to the right of **Routes** if entries must be made to the card routing table. The Routes fields expand (see Figure 69 on page 355).

Figure 69
Routes



Under **Routes**, enter the **IP address** and **Subnet mask** for any host that is not on the ELAN subnet but requires access to the Voice Gateway Media Card across the ELAN. A Telnet session for maintenance from a remote PC is an example of when this would be needed. The address of the remote PC would be added in the Route list.

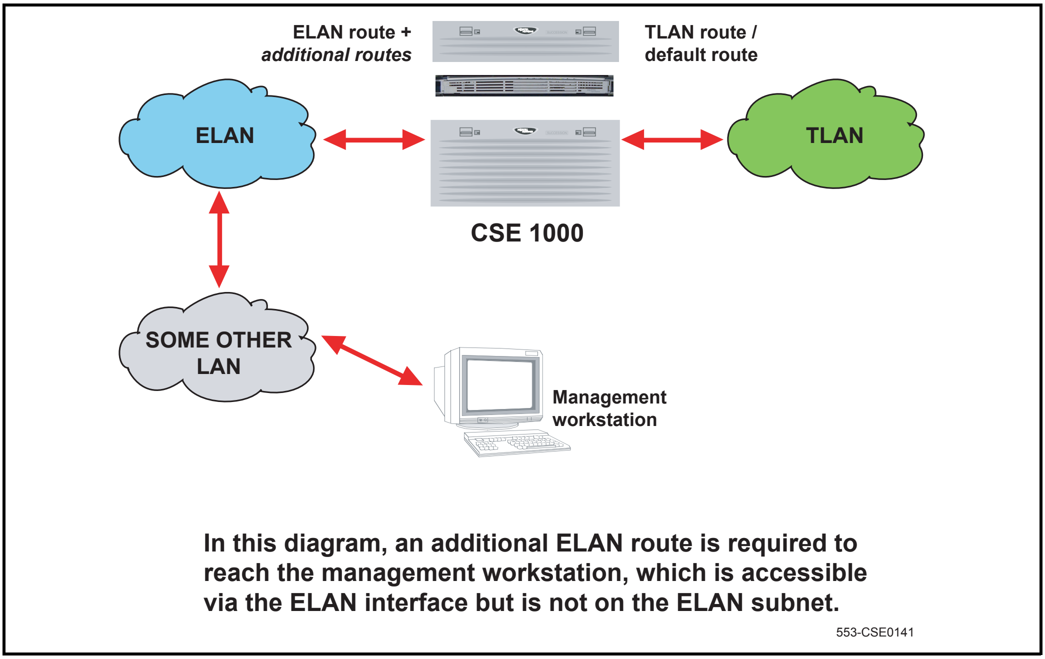
The default route on the card causes packets for unknown subnets to be sent out the TLAN interface. Packets from an external host arrive on the ELAN interface and responses are sent on the TLAN interface. This can cause one-way communication if the TLAN is not routed to the ELAN. It is necessary to add an entry in the Route list, to correct the routing so response packets are sent on the ELAN. Each entry creates a route entry in the card's route table that directs packets out the ELAN interface (see Figure 70 on page 357).

CAUTION

Use caution when assigning card routing table entries. Do not include the IP address of an Internet Telephone. Otherwise, voice traffic to these Internet Telephones is incorrectly routed through the ELAN and ELAN gateway. To avoid including the wrong IP address, it is recommended that Host IDs are defined for the card routing table entries.

5 To add additional routes, click the **Add** button again and enter the route information. Repeat this step for each route to be added.

Figure 70
Specifying additional ELAN routes



End of Procedure

Configuring File Server access

With the addition of new Internet Telephones, there are also additional firmware files for the Internet Telephones. The Voice Gateway Media Card has limited space to store the files on the card for all the telephones. As a result, a file server is used to store the telephone firmware files.

The Internet Telephone firmware files are labeled as follows:

- 0602Bnn.BIN is the filename for the i2004 Internet Telephone firmware where Bnn = F/W version 1.nn.
- 0603Bnn.BIN is the filename for the i2002 Internet Telephone firmware where Bnn = F/W version 1.nn.

If the external file server option is used in Element Management for firmware distribution with a node, the files must be renamed before being placed on the server:

- 0602Bnn.BIN must be renamed to i2004.fw
- 0603Bnn.BIN must be renamed to i2002.fw

To configure the file server, follow the steps in Procedure 39 on page 359.

Procedure 39
Configuring access to the file server

1 Click **Firmware** (see Figure 71).

Figure 71
Configuration > Node Summary > Edit > Firmware

2 Specify the parameters needed to connect to the file server:

a. **Firmware download server IP address:** Enter the IP address of the file server where firmware can be downloaded.

b. **Firmware file path:** Enter the path for the location of the firmware files. See page 104 for the default location of firmware files for the Succession CSE 1000 Rel 2.0 system.

c. **User ID:** Enter the User ID that is required to access the file server.

d. **Password:** Enter the Password that is required to access the file server.

End of Procedure

Configuring Loss and Level Plan

Loss and Level Plan determines parameters, such as transmission gain, that vary from country to country. Follow Procedure 40 on page 360 to configure the Loss and Level Plan.

Procedure 40
Configuring the Loss and Level Plan

1 Click **Loss Plan** (see Figure 72).

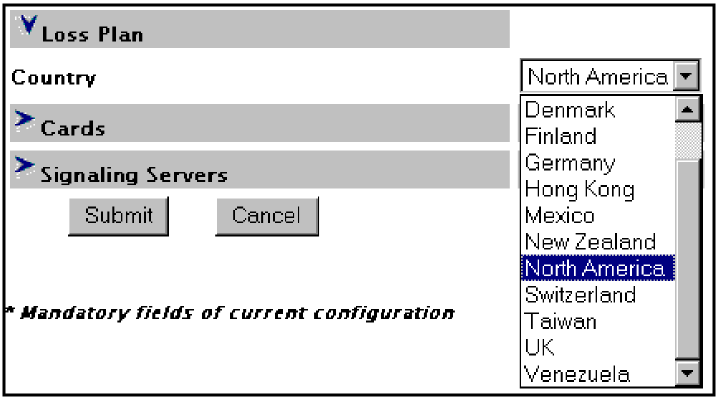
Figure 72
Configuration > Node Summary > Edit > Loss Plan

2 Select your **Country** from the pull-down box (see Figure 73 on page 361).

The Loss and Level Plan values are stored in a file in Element Management. Element Management reads the file to acquire the loss and level values for the selected country and places the values in a CONFIG.INI file on the Voice Gateway Media Cards.

Note: A dynamic loss plan has been implemented on the Succession CSE 000 Rel 2.0 system. It uses PDCA Table 15 in LD 73 to define the gateway loss value per endpoint connection type and adjusts the Voice Gateway Media Card gateway channel's loss for each call by sending pad values to the card. The default values in the system are for the North American loss plan. Installation of the Succession CSE 000 Rel 2.0 system in any other country requires setting the pad values in Table 15 to that country's loss plan. See the section on Transmission Parameters in *Planning and Engineering Guidelines* (553-3023-102) for details.

Figure 73
Loss Plan countries



End of Procedure

Configuring the card properties of the Voice Gateway Media Card

If the IP Network administrator provides IP addresses and subnet masks in CIDR format, for example, "10.1.1.10/24", convert the subnet mask to dotted decimal format. See Appendix D on page 675.

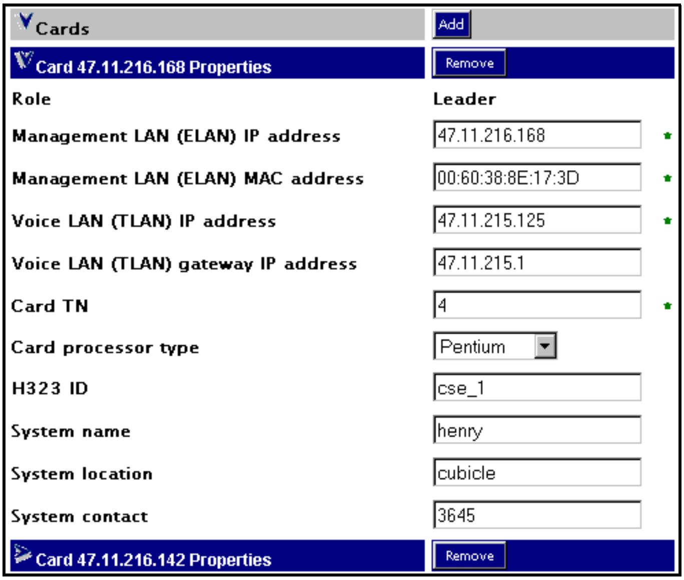
Note 1: In the Cards section, cards can be Added, Changed, or Removed in the node one at a time.

WARNING
Every node must has a Leader. Exercise caution when removing the Leader card. If the Leader card is deleted, a new Leader must be configured immediately.

Procedure 41
Configuring Voice Gateway Media Card properties

1 Click **Cards** and then click the **Add** button (see Figure 74).

Figure 74
Configuration > Node Summary > Edit > Cards



2 Enter the **Card Properties** data for Leader 0 and Follower cards. The fields with green asterisks are required fields:

a. **Role:** The role is assigned based on the information that Element Management reads from the card configuration. This is a read-only field.

b. **Management LAN (ELAN) IP address:** This is the ELAN IP address for the card. Element Management and Succession CSE 1000 use this address to communicate with the card.

c. **Management LAN (ELAN) MAC address:** This is the motherboard Ethernet address from the “Voice Gateway Media Card installation summary sheet” on page 209.

d. **Voice LAN (TLAN) IP address:** This is the TLAN IP address for the card.

e. **Voice LAN (TLAN) gateway IP address:** This is the IP address of the router interface on the TLAN.

f. **Card TN:** Enter the card slot number between 1-50.

g. **Card processor type:** Choose either Pentium or Succession Media Card. Select Pentium if using the ITG-P Line Card (dual-slot card). Select Succession Media Card if using MC (single-slot card).

h. **H323 ID:** The H323 ID within IP Line is for the Virtual Office/Branch Office feature. Keep the H323 ID the same for all the elements within one node.

i. **System name:** Enter the name of the system.

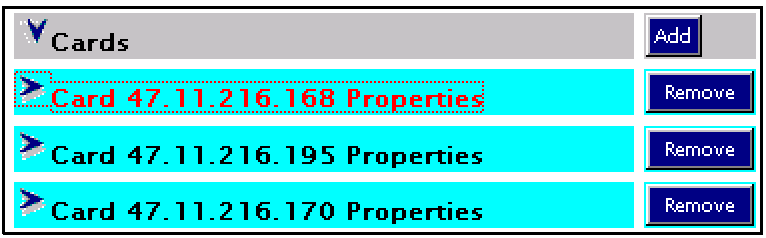
j. **System location:** Enter the location where the system resides.

k. **System contact:** Enter the system contact name and phone number.

3 To add additional cards to the node, click the **Add** button again and enter the new card information. Repeat this step for each card that is being added to the node.

4 New cards appear under the Cards menu as they are added (see Figure 75 on page 363).

Figure 75
Cards



End of Procedure

Submitting and transferring the node information

To submit node changes and transfer the changes to the Call Server, follow the steps in Procedure 42 on page 364.

Procedure 42
Submitting and transferring the node information

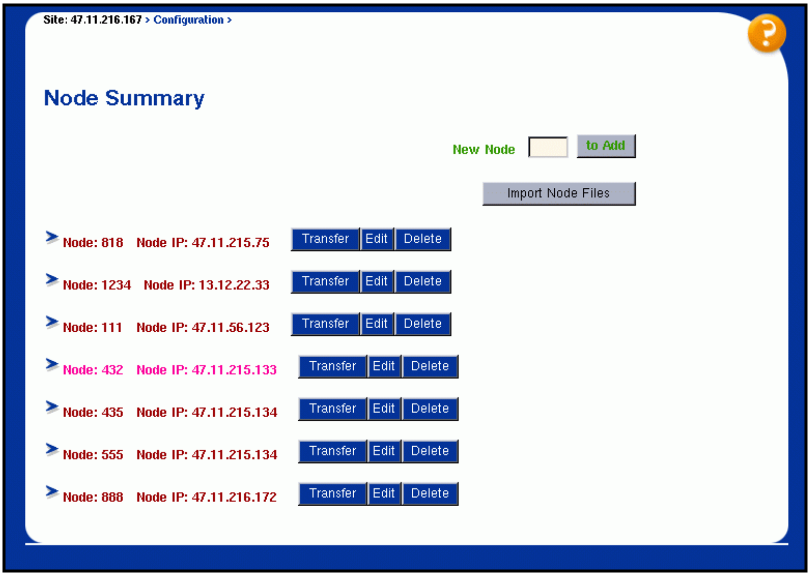
1 Click the **Submit** button when all the node information has been configured in the Edit page. Clicking the Submit button saves the data to the Call Server.

Note 1: The Submit button can be clicked after each section is configured in the Edit page. However, each time the Submit button is clicked, the Edit page closes and the Node Summary page is displayed. To continue the node configuration, click the Edit button to return to the Edit page.

Note 2: If the Cancel button is clicked, all information that has been configured is discarded. The Edit page closes and the Node Summary page opens.

The Edit page closes, and the Node Summary page opens with the new node added (see Figure 76 on page 365).

Figure 76
Node added to Node Summary page



Note: Three buttons are also added to the Node Summary page: **Transfer**, **Edit**, and **Delete**.

- The Transfer button is used to transfer the request to the node. The node then obtains its information (CONFIG.INI and BOOT.P files) from the Call Server.
- The Edit button retrieves the node information from the Call Server. The information is returned to the Edit page. The node information can then be changed.
- The Delete button is used to delete the node information from the Call Server.

2 Click the **Transfer** button.

3 Click **OK** to confirm the transfer (see Figure 77 on page 366).

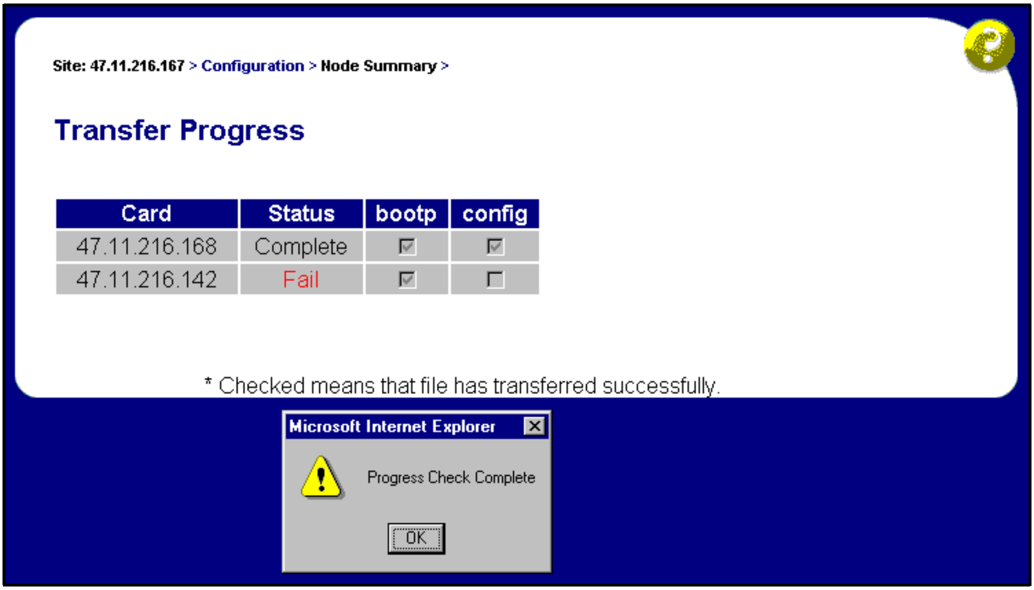
Figure 77
Transfer confirmation dialog box

4 After a few seconds, the **Transfer Progress** page opens and displays each of the Voice Gateway Media Card in the node (see Figure 78 on page 367).

The Voice Gateway Media Card's retrieve the CONFIG.INI and BOOTP.TAB files from the Call Server. A check mark is added to each field as the card receives its CONFIG.INI and BOOT>TAB files. When the transfer is complete, click **OK** in the Progress Check Complete dialog box.

- If the transfer is successful for a card, the Status column displays "Complete".
- If the transfer is unsuccessful, the Status column displays "Fail".

Figure 78
Transfer Progress page



End of Procedure

Transfer IP Telephony node configuration from Element Management to the Voice Gateway Media Cards

Before beginning, ensure the following:

- The Voice Gateway Media Cards and cables have been installed.
- The ELAN and TLAN interfaces of all cards are connected with access to the IP network.
- A PC is connected to a LAN that has access to the Signaling Server's node IP address, either directly or routed through the network so Element Management can run in a Web browser.

Overview

The IP Telephony node and card properties are configured using Element Management. The configuration data must be saved to the Call Server and then transferred to the Voice Gateway Media Cards.

The configuration data is saved when the Submit button on the Edit page is clicked. Submitting saves the files to the Call Server. After the data has been saved, the configuration must be transferred to the Voice Gateway Media Card. When the Transfer button on the Node Summary page is clicked, Element Manager instructs each card where to FTP the files from. The Voice Gateway Media Card then retrieves the CONFIG.INI and BOOTP.TAB files.

> ***Note:*** The following sequence of steps are applicable only to nodes that do not use the Signaling Server as the Leader card, that is a second (or subsequent) node configured on the system - not the main node. The Signaling Server must be properly configured to use Element Management, so the steps of setting Leader and rebooting the Leader are not needed. The Signaling Server requires a reboot only if the Signaling Server IP address information has been changed such as the Node IP address or Signaling Server TLAN IP address. The Voice Gateway Media Cards require a reboot only if the card IP address information has been changed.

For a Signaling Server node, the process consists of the following steps:

1 Transmit the node properties. See Procedure 44 on page 372.

2 Configure the Follower card. See Procedure 45 on page 375.

For a second (or subsequent) node, the process consists of the following steps:

1 Set the Leader IP address. See Procedure 43 on page 369.

2 Transmit the node properties. Procedure 44 on page 372.

3 Configure the Follower card. See Procedure 45 on page 375.

Setting the Leader IP address

Follow the steps in Procedure 43 to set the IP address of the Leader Voice Gateway Media Card.

Procedure 43
Setting the Leader IP address for a second or subsequent node

1 Access the IPL> CLI by connecting the COM port of a PC to the RS232 serial maintenance port on the faceplate of the Leader Voice Gateway Media Card with an NTAG81CA PC Maintenance cable. If required, use an NTAG81BA Maintenance Extender cable between the PC Maintenance cable and the PC.

Alternatively, connect the NTAG81BA Maintenance Extender cable to the female DB-9 connector of the NTMF94EA ELAN, TLAN RS232 Ports cable for a more permanent connection to the Voice Gateway Media Card serial maintenance port.

Note: Never connect two terminals to the faceplate and I/O panel breakout cable serial maintenance port connectors at the same time.

2 Use the following communication parameters for the TTY terminal emulation on the PC: 9600 baud, 8 bits, no parity, one stop bit.

3 Observe the Leader card faceplate maintenance display window.

When the display reads "T:20", it begins to send BootP requests on the ELAN. A series of dots is printed on the TTY.

4 Type **+++** to escape from the BootP request.

5 At the Login prompt, enter the userid and password to access the IPL> CLI:

- If it is a new card (out of the box), then the userid is itgadmin and the password is itgadmin
- If it is a card which has been previously connected to the Call Server, then the userid and password is the PWD1 of the Call Server.
- If the userid and password are forgotten, see Procedure 57 on page 417 to reset the IPL> CLI Shell username and password.

6 When the maintenance window displays "T:21", login to the IPL> CLI. At the IPL> prompt, enter the setLeader command to set the Leader Management LAN IP address, Management LAN gateway IP address and the Management LAN subnet mask:
setLeader “xx.xx.xx.xx”,“yy.yy.yy.yy”,“zz.zz.zz.zz”

Note 1: The three parameters must each be enclosed in double quotation marks. Ensure that there is a space after the command and before the first parameter. Put commas and no spaces between the following parameters:

“xx.xx.xx.xx”=IP address.
Enter the same IP address that was entered in the **Management LAN IP address** field for **Leader** in the **Cards** menu of the **Edit** page.

"yy.yy.yy.yy"=Gateway IP address.
Enter the same address that was entered in the **Management LAN gateway IP address** field in the **Node** menu of the **Edit** page. If there is none, enter the following: "**0.0.0.0**"

"zz.zz.zz.zz"=Management LAN subnet mask.
Enter the same address that was entered in the **Management LAN subnet mask** field **Node** menu of the **Edit** page.

Note 2: This step assumes that the new IP Telephony node has already been configured in Element Management

7 Reboot the Leader Voice Gateway Media Card. At the IPL> prompt, enter: **cardReset**, or press the Reset button on the faceplate of the Leader Voice Gateway Media Card.

> **WARNING**
> Do not use a pencil to reset the Voice Gateway Media Card. The graphite carbon can create an electrical short circuit on the board.

8 Check the maintenance display for T:22 to confirm a successful reboot.

9 In Element Management, click **System Status > IP Telephony**. The **IP Telephony Information** pages opens. Expand the node. Click the Leader card's **Status** button to check the status of the card. Otherwise, verify LAN connections and IP configuration.

End of Procedure

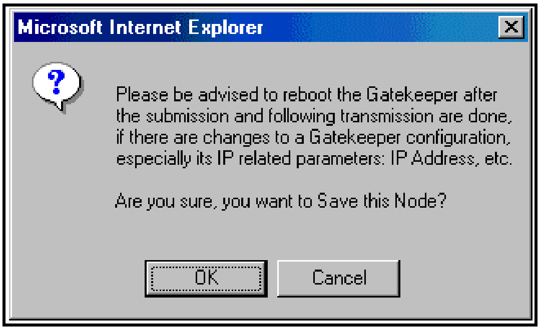
Transmitting node properties

To transmit the node properties to Leader, follow the steps in Procedure 44.

Procedure 44
Transmitting node properties to Leader

1 If changes are made to the node or card configuration data, ensure the data is saved to the Call Server by clicking the **Submit** button. A confirmation dialog box appears (see Figure 79).

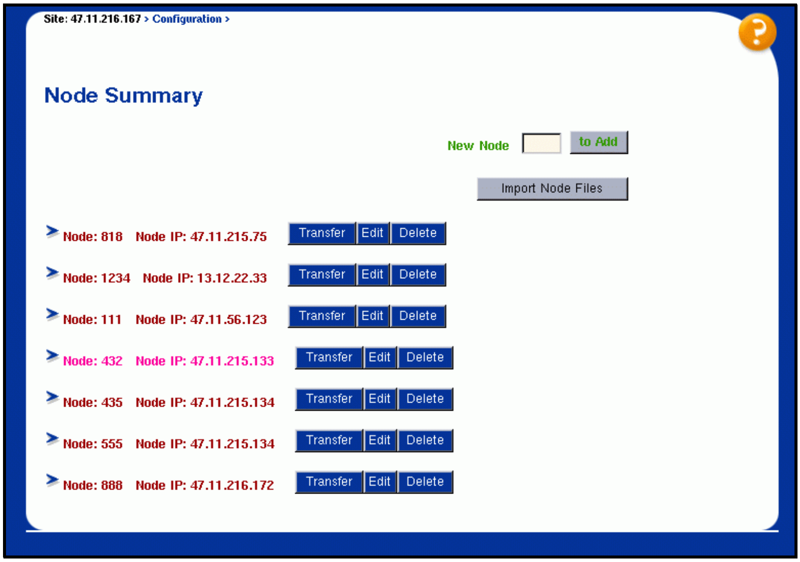
Figure 79
Confirm Submit



2 Click the **OK** button to confirm the save of the node data.

3 The Edit page closes, and the Node Summary page opens. In the Node Summary page, click the **Transfer** button associated with the node (see Figure 80 on page 373).

Figure 80
Transfer Node



4 Click the **Transfer** button. Click **OK** to confirm the transfer (see Figure 81).

Figure 81
Transfer confirmation dialog box

5 Element Management notifies the Leader and the Voice Gateway Media Card's then retrieve the CONFIG.INI and BOOTP.TAB files from the Call Server.

The **Transfer Progress** page opens and displays each of the Voice Gateway Media Card in the node. The Voice Gateway Media Card's retrieve the CONFIG.INI and BOOTP.TAB files from the Call Server. When the transfer is complete, click **OK** (see Figure 78 on page 367) in the Progress Check Complete dialog box. If the transfer is successful for a card, the Status column displays "Complete." If the transfer is unsuccessful the Status column displays "Fail."

6 The Leader card must be reset, if the Leader card:

- is a new card (out of the box)
- is a card that is being configured for the first time as a Leader card
- has had a change to Leader's IP address information

In the Navigation Tree, click System **Status > IP Telephony**. The IP Telephony Information pages opens. Click the **Reset** button associated with the Leader card.

Note 1: If any of the Signaling Server IP address information is changed, the Signaling Server must be rebooted.

Note 2: The cards can also be restarted by entering the **cardReset** command at the IPL> prompt or by pushing the Reset button on the card's faceplate.

WARNING
Do not use a pencil to reset the Voice Gateway Media Card. The graphite carbon can create an electrical short circuit on the board.

End of Procedure

Configuring the Follower cards

To configure the Follower card, follow the steps in Procedure 45 on page 375.

Procedure 45
Configuring the Follower cards

1 Check the displays on the card faceplate.

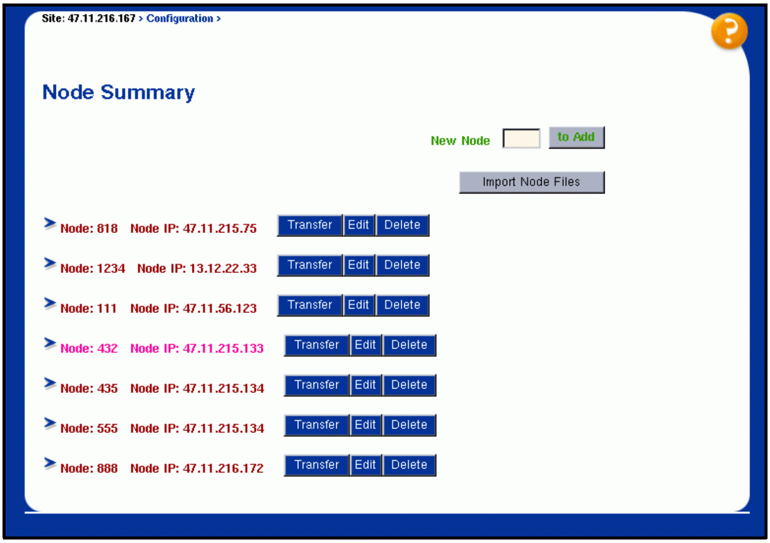
- After successfully rebooting, the Leader card is now fully configured with the Node Properties of the node and enters a state of “active Leader”. The Card faceplate display shows Lxxx, where xxx = the number of Internet Telephones registered with the terminal proxy server on the Leader card. L000 shows that no Internet Telephones are registered.
- The Follower cards receive their BOOTP configuration information from the Leader card. The Follower faceplate display shows Fxxx, where xxx = the number of Internet Telephones registered with the Follower’s terminal proxy server. F000 shows that no Internet Telephones are registered.

2 Reboot the Follower card if the card’s faceplate does not display FXXX or F000.

3 Once all the cards have the correct display on their faceplates, go to Element Management.

4 In the Node Summary page, click the **Transfer** button associated with the node (see Figure 80 on page 373).

Figure 82
Transfer Node



5 Click the **Transfer** button. Click **OK** to confirm the transfer (see Figure 81 on page 373).

Figure 83
Transfer confirmation dialog box

6 The **Transfer Progress** page opens and displays each of the Voice Gateway Media Card in the node. The Voice Gateway Media Card's retrieve the CONFIG.INI and BOOTP.TAB files from the Call Server. When the transfer is complete, click **OK** (see Figure 78 on page 367) in the Progress Check Complete dialog box. If the transfer is successful for a card, the Status column displays "Complete." If the transfer is unsuccessful the Status column displays "Fail."

7 If the Follower card is new card (out of the box), then reboot the card.

End of Procedure

Upgrade the Voice Gateway Media Card loadware and Internet Telephone firmware

Before upgrading the card loadware and the Internet Telephone firmware, check the version of card loadware and firmware that is currently installed. Compare this to the latest versions available by accessing the Nortel Networks Web site. When a loadware or firmware upgrade is required, go to the Nortel Networks Web site to download the appropriate upgrade files.

Before beginning, ensure that the following software is installed on the PC:

- Software to extract zipped files (WinZip or equivalent)
- A Web browser (such as Microsoft Internet Explorer or Netscape Navigator)

The following steps are required to upgrade the Voice Gateway Media Card loadware and Internet Telephone firmware:

1 Check the version of the loadware currently installed on the Voice Gateway Media Card (see Procedure 46 on page 381).

2 Check the version of the firmware that is currently running on the Voice Gateway Media Card (see Procedure 47 on page 383).

3 Download the most up-to-date version of the loadware and firmware files from the Nortel Networks Web site (see Procedure 111 on page 719).

4 Upload the loadware and firmware files using the File Upload system utility in Element Management (see Procedure 49 on page 388).

5. Upgrade the Voice Gateway Media Card loadware (see Procedure 50 on page 389).

6. Restart the Voice Gateway Media Card (see Procedure 51 on page 393).

7. Upgrade and distribute the Internet Telephones firmware on the Voice Gateway Media Card (see Procedure 52 on page 394).

   Note: To upgrade the Voice Gateway Media Card firmware, see Procedure 53 on page 401.

Once the Voice Gateway Media Card loadware and i2002/i2004 Internet Telephone firmware has been verified, there are three upgrade options:

1. Upgrade the Voice Gateway Media Card loadware only. It may only be necessary to upgrade the Voice Gateway Media Card loadware. This option is used most frequently; however, verify if an Internet Telephone firmware upgrade is also required.

2. Upgrade both the Voice Gateway Media Card loadware and the i2002/i2004 Internet Telephone firmware. Both the Voice Gateway Media Card loadware and the i2002/i2004 Internet Telephone firmware may need to be upgraded.

   Note: Defer restarting the cards until the end of the firmware upgrade. If the Internet Telephones are registered to the Signaling Server, rebooting the Voice Gateway Media Card does not affect the telephones as long as they are not using a gateway channel on the rebooted card. However, if the Internet Telephones are registered to the Voice Gateway Media Card, resetting the card causes the Internet Telephone to reboot and reregister.

3. Upgrade only the i2002/i2004 Internet Telephone firmware. It may only be necessary to upgrade the i2002/i2004 Internet Telephone firmware.

   Note: In this case, restart all the telephones instead of the Voice Gateway Media Cards. To do this, select a single test telephone and reset the firmware only on that test telephone before completing the procedure on all telephones. If the upgrade works properly, use the umsUpgradeAll command to complete the upgrade on all the telephones.

i2002 and i2004 Internet Telephone firmware requirements

The i2002 and i2004 Internet Telephone firmware can be upgraded in the field. With the introduction of IP Line 3.0, the number of Internet Telephones has increased. As a result of this increase there is also an increase in the number of firmware versions for the Internet Telephones. There is one firmware file for each type of Internet Telephone.

In the past, a copy of the firmware was stored on each card in the system to automatically upgrade Internet Telephones if an upgrade is required. There is limited space on the Voice Gateway Media Card (running IP Line 3.0) to store the firmware files. Therefore, the firmware is stored on a file server or on the Master card’s RAM device.

If a file server is used to store the firmware file, the following items are required to access the firmware:

- IP address of the file server
- Routing table
- File path to the file server
- User name and password required to access the files server

This information is configured in Element Management under Firmware on the Edit page (see Figure 71 on page 359).

- For a node using the Signaling Server as the Leader, no Firmware Server configuration is necessary since the files are stored on the Signaling Server and by default, the files are retrieved from the Signaling Server.
- For nodes that are not using the Signal Server as the Leader, configure the FTP access information for the Signaling Server or some other server as the Firmware server.

The i2004 and i2002 Internet Telephones use Trivial File Transfer Protocol (TFTP) to transfer the firmware; therefore, the customer’s network must support TFTP. For example, the customer's network cannot have telephones on the other side of a firewall that blocks the TFTP port number.

Default location of firmware files

The default location of the firmware files is different depending on the system configuration, due to limitations of the various platforms:

- Normal CSE 1000 Rel 2.0:
  - — The firmware file is stored on the Signaling Server in the "/u/fw" directory.
- Node using a Voice Gateway Media Card as the Leader card (the files can be located in any of the following locations):
  - — The firmware files can be retrieved from the system's Signaling Server.
  - — The files can be placed on a PC Card plugged into the Leader's faceplate.
  - — The files can be placed on an alternate file server.

Internet Telephone Firmware upgrade from a new Voice Gateway Media Card

Use Element Management to upgrade the Internet Telephone firmware files to the new Voice Gateway Media Card (see Procedure 52 on page 394).

Verifying Voice Gateway Media Card loadware

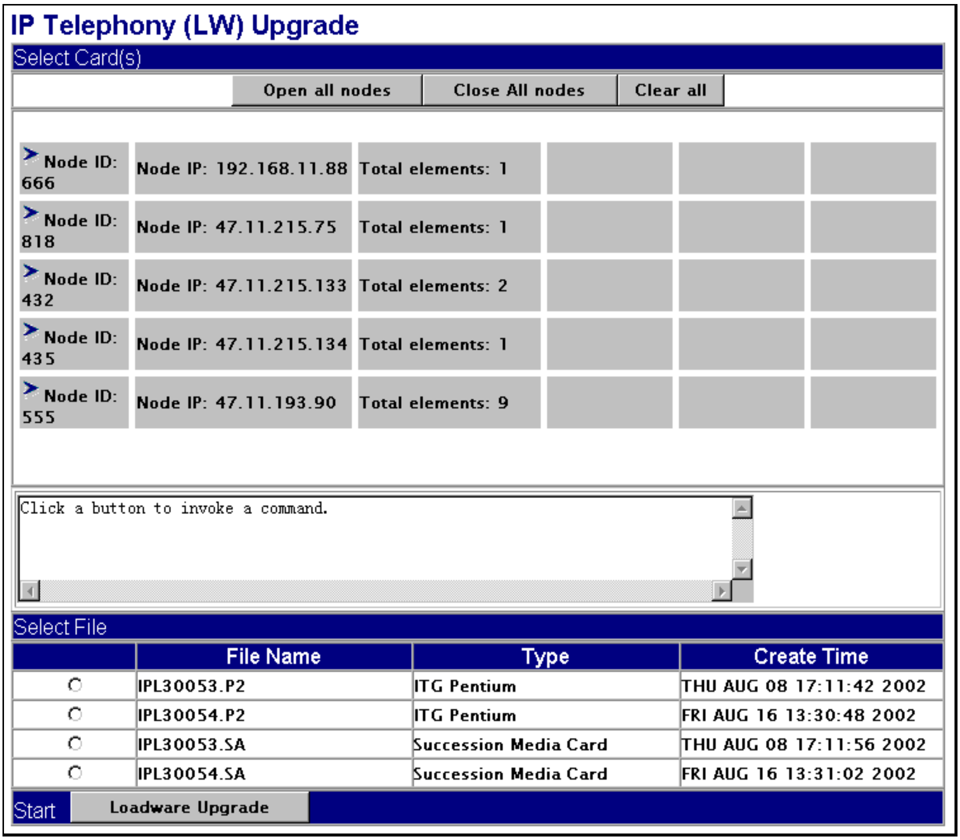
To check the version of loadware on the Voice Gateway Media Card, follow the steps in Procedure 46 on page 381.

Procedure 46
Verifying card loadware

1 Click **Software Upgrade** from the Navigation Tree.

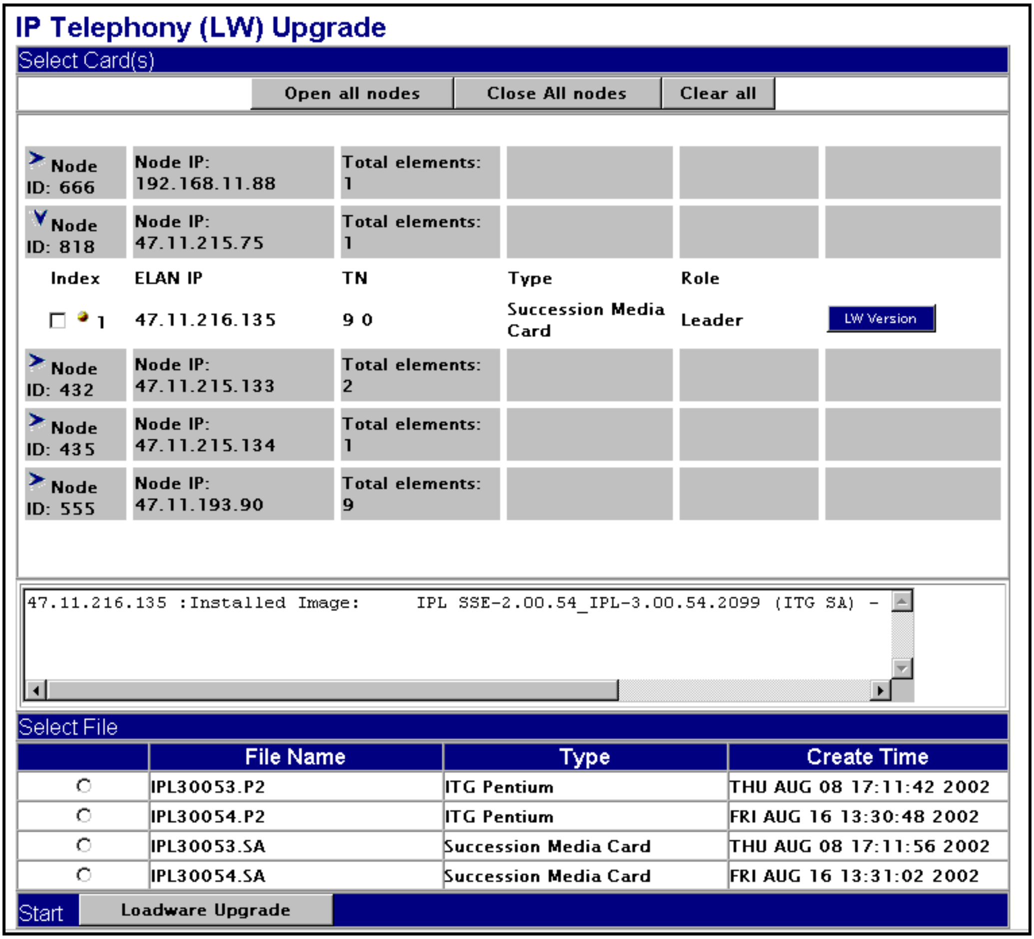
2 Click **IP Telephony(LW)** from the expanded Software Version menu. The **IP Telephony (LW) Upgrade** page appears (see Figure 84 on page 381).

Figure 84
IP Telephony (LW) Upgrade



3 Expand a node and select a card in the node (see Figure 85 on page 382).

Figure 85
LWVersion



4 Click the **LWVersion** button located to the right of the card information.

The loadware version running on the card is displayed in the pane in the center of the IP Telephony (LW) page (see Figure 85 on page 382)

5 Note the loadware version for the card.

End of Procedure

Verifying the Internet Telephone firmware

To check the version of firmware on the Voice Gateway Media Card, follow the steps in Procedure 47 on page 383.

Procedure 47
Verifying the Internet Telephone firmware

1 Click **Software Upgrade** from the Navigation Tree.

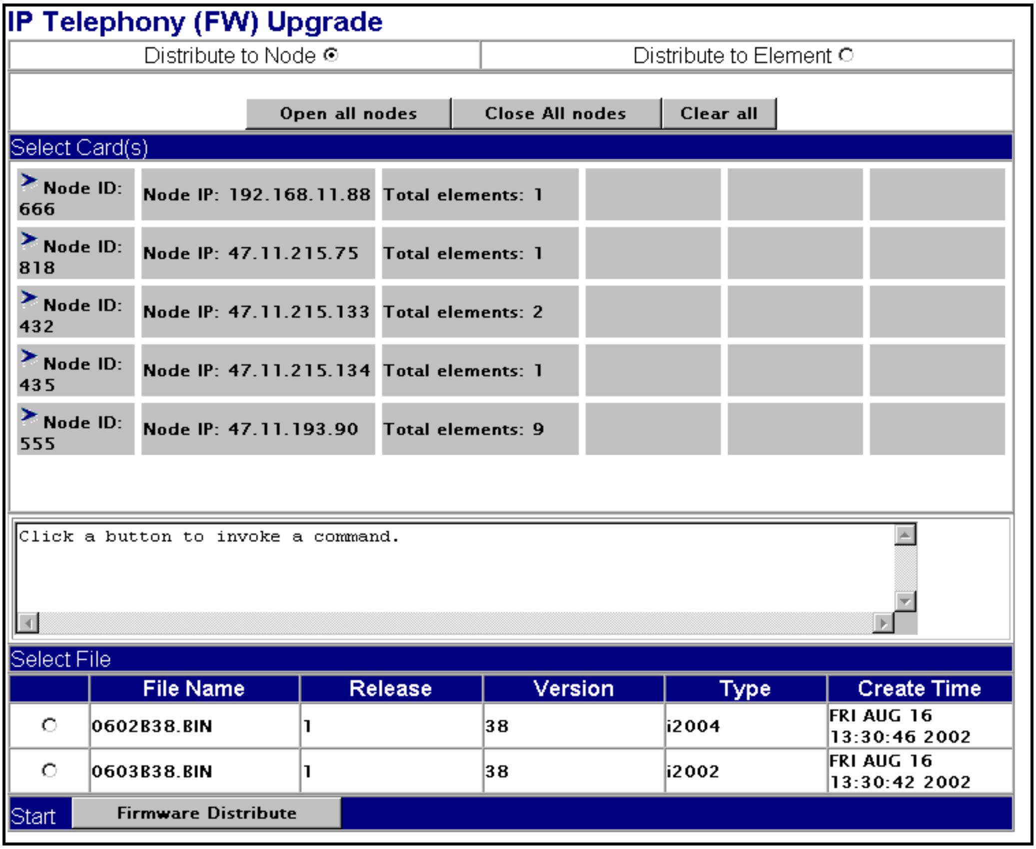
2 Click **IP Telephony(FW)** from the expanded Software Version menu. The **IP Telephony (FW) Upgrade** page appears (see Figure 86 on page 384).

At the top of the screen, there are two radio buttons:

i. **Distribute to Node** - Disables all elements that are not Leaders. Distribute to Node is the default since IP Line is responsible for distributing from the Leader to all followers in a node.

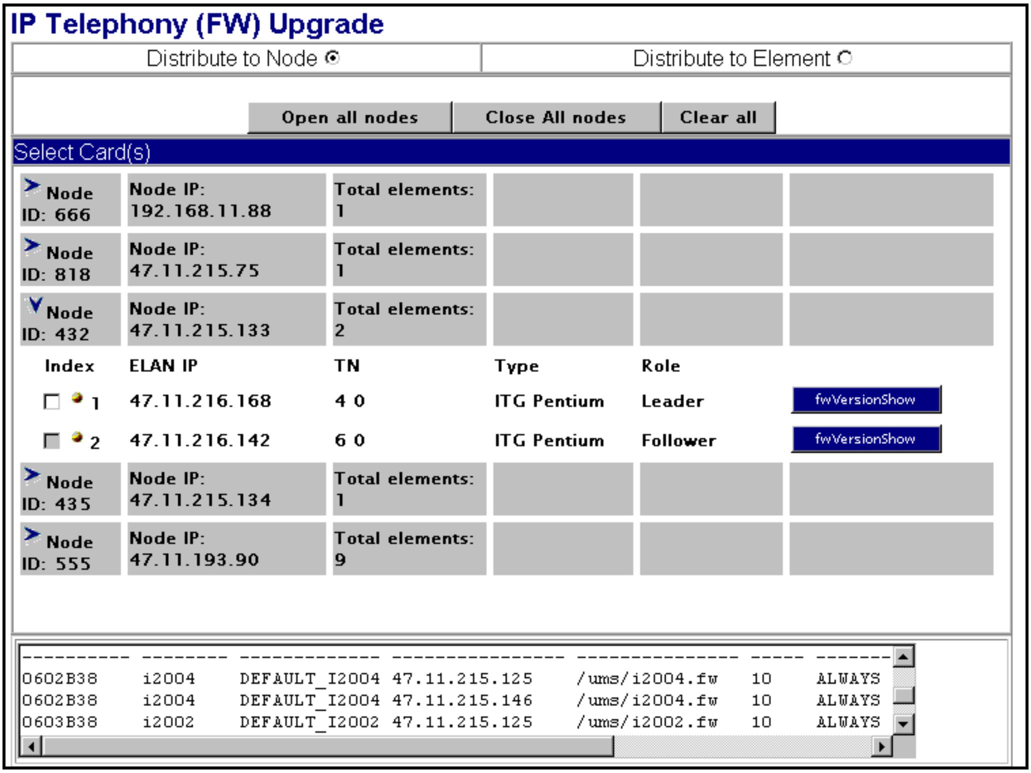
ii. **Distribute to Elements** - Enables all the elements in case the user needs to distribute the firmware to some elements which have failed.

Figure 86
IP Telephony (FW)



3 Expand a node and select a card (see Figure 87 on page 385).

Figure 87
FWVersionShow



4 Click the **fmVersionShow** button located to the right of the card information.

The firmware version running on the card is displayed in the pane in the center of the IP Telephony (FW) page.

5 Note the firmware version for the card.

End of Procedure

Downloading the current loadware and Internet Telephone firmware

To check for the latest loadware and firmware releases on the Nortel Networks Customer Support Web site, follow the steps in Procedure 48 on page 386.

Procedure 48
Downloading loadware and firmware from the Nortel Networks Web site

1 Check the Nortel Networks Customer Support Web site for the latest IP Line loadware and Internet Telephone firmware releases. Download the **2.00.xx Signal Server CD Image** file. See Procedure 111 on page 719 for the steps for downloading files from the Nortel Networks Web site.

Note: The IP Line loadware and Internet Telephone firmware files are contained in the **2.00.xx Signal Server CD Image** file in the "**Succession Communication Server for Enterprise 1000**" product list on the Nortel Networks Web site. The file contains:

- The **IPL300xx*.p2** and **IPL300xx*.sa** loadware files. The IPL300xx*.p2 file is the IP Line application for the ITG-P Line Card and the IPL300xx*.sa is the IP Line application for the Succession Media Card.
- The **0602Bxx.BIN** (i2004) and **0603Bxx.BIN** (i2002) firmware files.

  For example, a firmware version can be labelled 0602B38 or 0603B38. This means Internet Telephone firmware version 1.38.

  — The 02 represents the i2004 Internet Telephone and 03 is the i2002 Internet Telephone.

  — The letter B represents the Version number 1.

  — 38 represents the Release number .38.
- A **readme.txt** file. The readme.txt file explains important considerations for installing the new loadware and firmware versions. The readme file also includes identifying information for the loadware and firmware files such as the date and time, size and checksum.

2 Compare the latest loadware and firmware versions available with the loadware and firmware version currently installed on the Voice Gateway Media Card and the Internet Telephones.

End of Procedure

Uploading the loadware and firmware files to the file server

The next step is to upload the files from the Element Management PC to the file server. The "Centralized file upload" page enables a user to upload and store loadware and firmware on the Signaling Server. These files can then be downloaded to the Internet Telephones and the Voice Gateway Media Cards using the loadware and firmware upgrade functions available from the Software Upgrade menu. The Signaling Server can be used as a central distribution point to load and activate loadware, firmware and patches. To upload the files, follow the step in Procedure 49 on page 388.

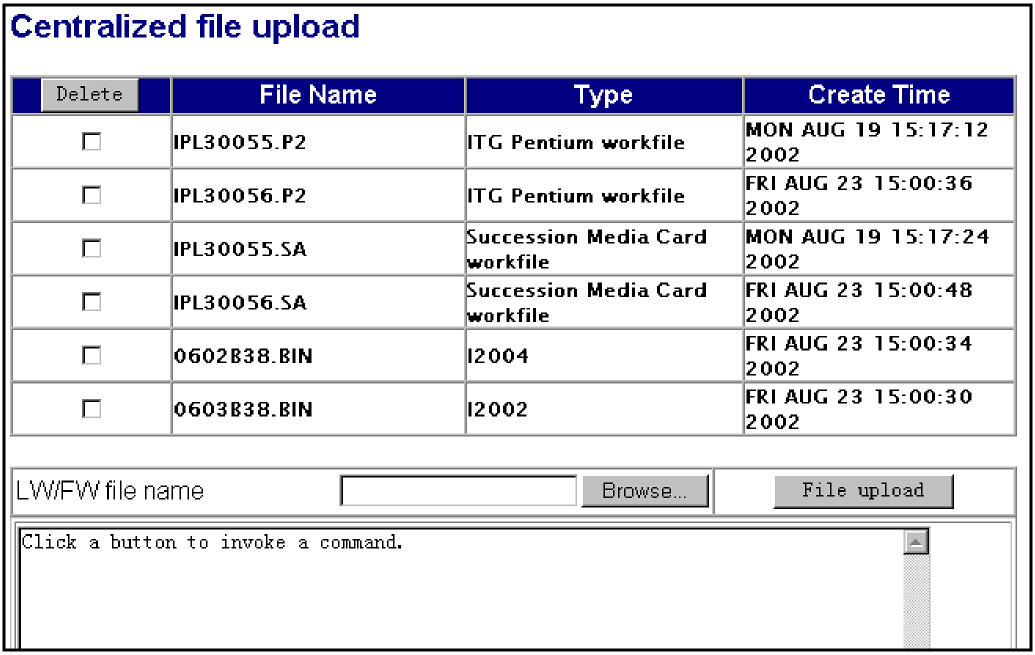
Note: For patches, Element Management does not need to upload to Signaling Server first. It gets the patch file from Element Management PC directly.

Procedure 49
Uploading loadware and firmware files

1 Click **Software Upgrade** in the Navigation Tree.

2 Click **File Upload**. The **Centralized file upload** page opens (see Figure 88 on page 388).

Figure 88
System Utility > File Upload > Centralized file upload



3 Click the **Browse** button. In the **Choose File** dialog box, select the path and file to upload. Alternatively, the user can enter the path and filename for the file to be uploaded.

Note: Only one loadware or firmware file can be uploaded at a time.

4 Once selected, the path and file name appear in the text box to the left of the Browse button (see Figure 89 on page 389).

Figure 89
Firmware file text box

5 Click the **File Upload** button.

6 The firmware file appears in the list at the top of the page when they are uploaded.

Note: To delete older versions of the firmware and loadware files, click the check box associated with the older file and then click the **Delete** button located at the top of the column of check boxes.

End of Procedure

Upgrading the Voice Gateway Media Card loadware

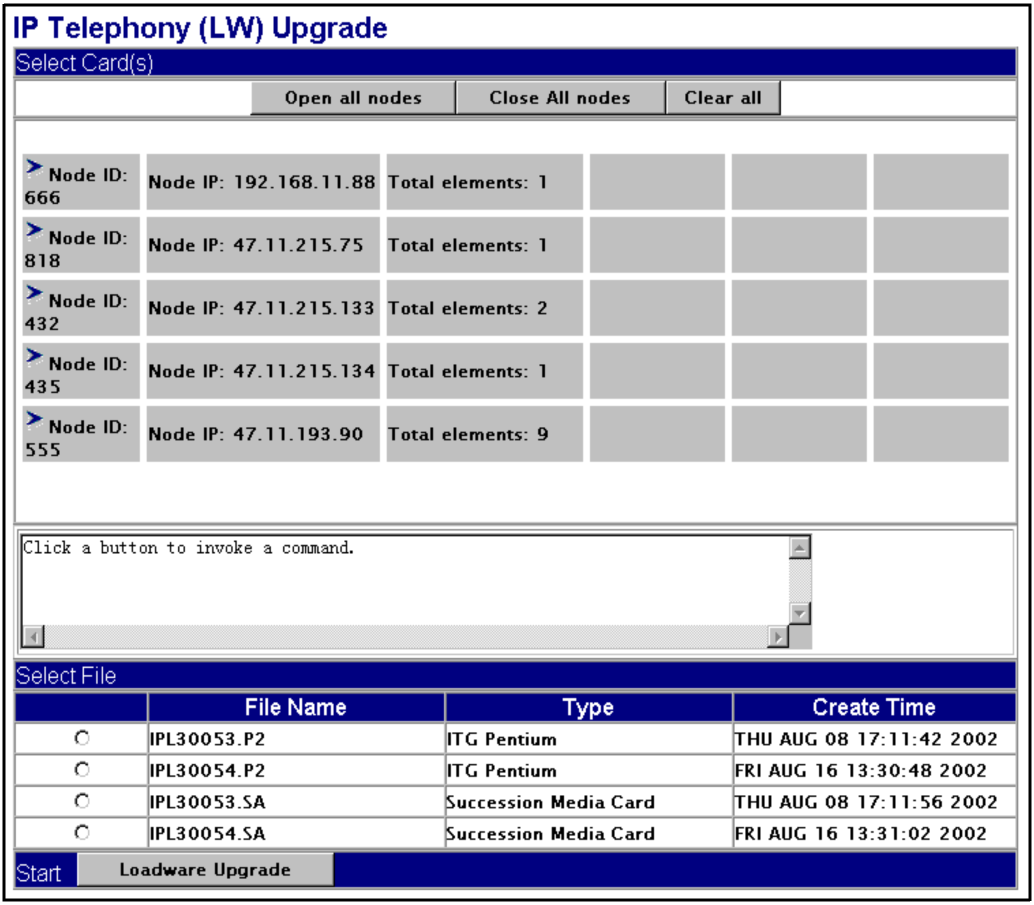
Once the files are uploaded to the file server, the cards must be upgraded to the newest loadware version. To upgrade the card loadware, follow the steps in Procedure 50 on page 389.

Procedure 50
Upgrading the card loadware

1 Click **Software Upgrade** from the Navigation Tree.

2 Click **IP Telephony(LW)** from the expanded Software Version menu. The IP Telephony (LW) Upgrade page appears (see Figure 90 on page 390).

Figure 90
IP Telephony(LW)



3 Expand a node.

4 Select the card(s) to upgrade, by clicking the check box to the left of the card information.

Note: Element Management can support upgrading the loadware on up to four cards at the same time.

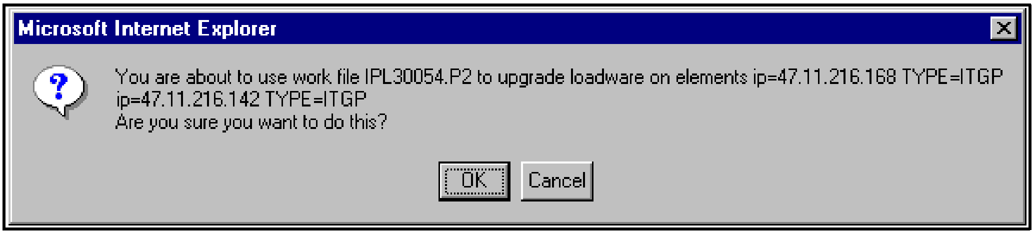
5 In the lower part of the page, click the radio button associated with the most current version of the loadware.

Note: If the card receiving the upgrade is of type ITG Pentium, select the radio button associated with the most current version of the ITG Pentium loadware (IPL300xx.P2). If the card receiving the upgrade is a Succession Media Card, select the radio button associated with the must current version of the Succession Media Card loadware (IPL300xx.SA).

6 Click the **Loadware Upgrade** button at the bottom of the page.

A confirmation dialog box appears similar to Figure 91 on page 391. Click **OK** to confirm the card upgrade. The upgrade begins.

Figure 91
Loadware Upgrade confirmation dialog box



7 The **Loadware Upgrade Progress** pages appears (see Figure 92 on page 392). The status of the upgrade is shown for each of the cards selected to receive the loadware upgrade. This status of the upgrade can be Work in progress, Upgrading, Fail, or Finished (see both Figure 92 on page 392 and Figure 93 on page 392).

Figure 92
Loadware Upgrade Progress - Upgrading Loadware

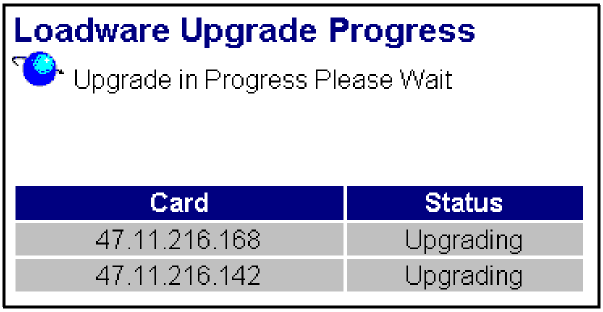
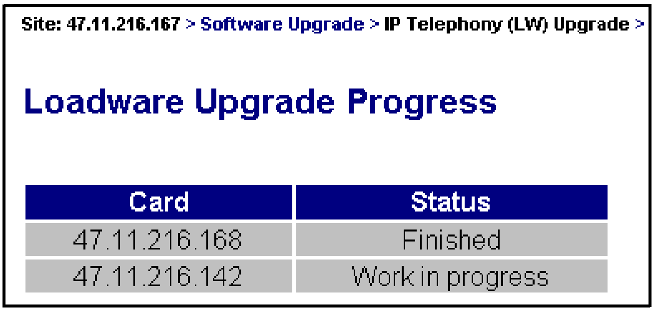


Figure 93
Loadware Upgrade Progress



8 Click **OK** to clear Progress Check Complete dialog box.

9 Repeat the above steps for the other card(s) that have to be upgraded.

End of Procedure

Rebooting the Voice Gateway Media Card

Follow Procedure 51 on page 393 to reboot a Voice Gateway Media Card.

Procedure 51
Rebooting the Voice Gateway Media Card

1 Disable the Voice Gateway Media Card.

2 Click **System Status** and then **IP Telephony**. The IP Telephony Information pages opens. Expand the node containing the card to be rebooted.

3 Click the **Reset** button to reboot the card.

Note 1: The cards remain in the "Disabled" state after the upgrade, so that the technician can issue a "Reset" command. The cards can also be reset by using a pointed object to press the Reset button on the card's faceplate.

Note: Reboot the Leader card only if the node is using the Voice Gateway Media Card as the Leader (that is, the Signaling Server is not the Leader).

4 Click the card's **Status** button in the IP Telephony Information page to verify the status of the Voice Gateway Media Card.

5 Use the LD 32 **ENLC** command to re-enable the Voice Gateway Media Cards.

6 Repeat these steps for each Voice Gateway Media Card that received the loadware upgrade.

End of Procedure

Upgrading the Internet Telephone firmware

When the IP Line 3.0 loadware has been upgraded, you must verify if an Internet Telephone firmware upgrade is also required. Check the Release Notes for the IP Line 3.0 application to determine which Internet Telephone firmware version is required to be compatible.

Once the files are uploaded to the file server, the cards must be upgraded to the newest Internet Telephone firmware version. To upgrade the firmware on the i2002/i2004 Internet Telephone, follow the steps in Procedure 52 on page 394. This procedure has two major steps:

- placing the Internet Telephone firmware onto each card in the node
- propagating the firmware from the card to each telephone registered on that card

Procedure 52
Upgrading the Internet Telephone firmware

1 Verify that all Voice Gateway Media Cards that require a firmware upgrade have established a signaling link with the Call Server.

Note: You first need to disable Voice Gateway Media Cards to update the firmware. Use the LD 32 DISI command to disable the card.

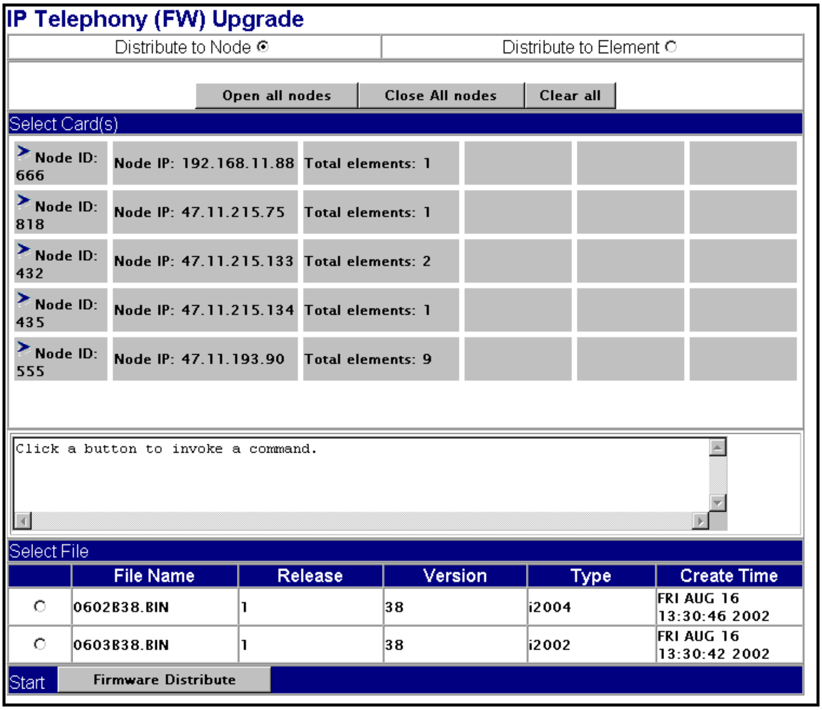
To verify the link is available between the PBX and card, Telnet to each card and login. From the command line, type **pbxLinkShow**. The status of the PBX link appears. If the link is active the page displays the following:

RUDPLinkState = Up

2 Click **Software Upgrade** from the Navigation Tree.

3 Click **IP Telephony(FW)** from the expanded Software Version menu. The IP Telephony (FW) Upgrade page opens (see Figure 94 on page 395).

Figure 94
IP Telephony (FW)



4 Expand the node containing the cards to receive the Internet Telephone firmware upgrade.

5 Select the card(s) to upgrade, by clicking the check box to the left of the card information.

Note: Element Management can support upgrading the firmware on up to four cards at the same time.

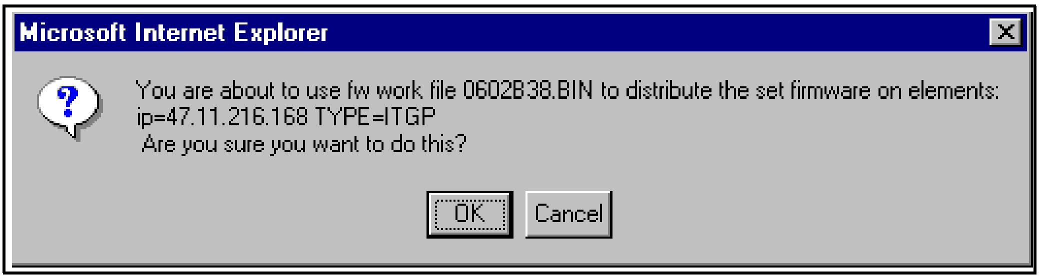
6 In the lower part of the page, click the radio button associated with the most current version of the firmware. Click the **Firmware Distribute** button. This step must be completed for each version of the firmware that has to be distributed.

CAUTION
Downloading an incorrect version of the Internet Telephone firmware can result in extended service interruptions and can require special recovery procedures.

7 A confirmation dialog box appears similar to Figure 95 on page 396.

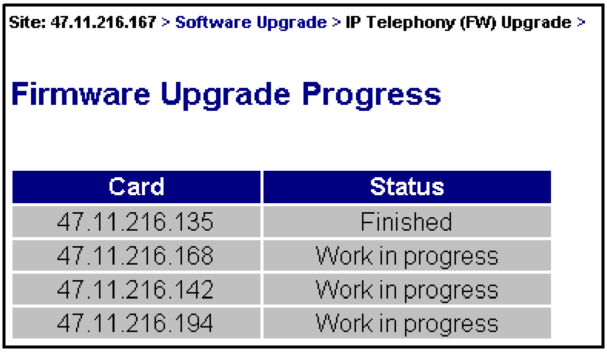
Click **OK** to confirm the firmware upgrade to the card. The upgrade begins.

Figure 95
Firmware Upgrade confirmation dialog box



8 The **Firmware Upgrade Progress** page opens (see Figure 96 on page 397). The status of the upgrade is shown for each of the cards selected to receive the firmware upgrade.

Figure 96
Firmware Upgrade Progress


Site: 47.11.216.167 > Software Upgrade > IP Telephony (FW) Upgrade >

Firmware Upgrade Progress

Card	Status
47.11.216.135	Finished
47.11.216.168	Work in progress
47.11.216.142	Work in progress
47.11.216.194	Work in progress

9 Repeat the above steps for the card(s) that have to be upgraded.

The Internet Telephones continue to run the old firmware until each telephone re-registers with a Voice Gateway Media Card that contains the new Internet Telephone firmware.

Note: Commands are available from the IPL> command line to upgrade a single i2002/i2004 Internet Telephone immediately, all i2002/i2004 Internet Telephones immediately, or schedule all i2002/i2004 Internet Telephones to be upgraded at a later time. Before doing this, verify that each card has the correct firmware version.

10 Select an Internet Telephone for test purposes.

11 Telnet to the card and then login to the IPL> command line, and enter the following:

isetReset "xxx.xxx.xxx.xxx"

where xxx.xxx.xxx.xxx is the IP Address of the selected telephone.

12 Monitor the display on the test telephone. As it upgrades the firmware, note the IP Address from which Voice Gateway Media Card it is receiving its upgrade.

13 Press the **Services** key (key with globe with arrow pointing East and West) on the i2002/i2004 Internet Telephone. The Services key enables you to access the **Telephone Options** list.

  i. Press **Select** to select Telephone Options.

  ii. Use the **Navigation** keys to scroll to **Set Info**.

  iii. Press the **Select** softkey, then press the **Navigation** keys until it displays **FW Version:**. For the Voice Gateway Media Card, select the appropriate firmware.

Note: For example, a firmware version can be labelled 0602B38 or 0603B38, and this means Internet Telephone firmware version 1.38.

- 02 represents the i2004 Internet Telephone and 03 represents the i2002 Internet Telephone.
- B represents the Version number 1.
- 38 represents the Release number .38.

14 Lift the handset and make a call to verify the telephone works.

15 Before proceeding, ensure the time on the card is set correctly. Telnet to each Voice Gateway Media Card and login. At the IPL> command line, enter the following:

```
umsUpgradeAll "hh:mma/p"
```

hh:mma/p specifies the time when the upgrade will occur, **a** represents A.M., and **p** represents P.M. The time is in Standard format.

For example, umsUpgradeAll “11:30a” or umsUpgradeAll “2:45p”.

At the time specified, all the i2002/i2004 Internet Telephones on the Voice Gateway Media Card go out of service. This can take several minutes.

Upon completion of the firmware upgrade, the i2002/i2004 Internet Telephones are brought back online in groups of ten.

CAUTION

The umsUpgradeAll command (without the time parameter) causes the i2002/i2004 Internet Telephones registered on all cards you are logged into to be immediately taken out of service, unless the time parameter is specified.

After the test telephone is working, the umsUpgradeAll does not need the time parameter. However, without the time parameter, the command immediately resets all the i2002/i2004 Internet Telephones currently registered on that line card.

If you do not immediately want to reset all the phones and you wish to schedule the reset time of the i2002/i2004 Internet Telephones, check the time on all the cards. Reset the time, if necessary, to ensure all cards have the same time, and then issue the umsUpgradeAll "hh:mma/p", where "hh:mma/p" represents the time when you want to schedule the upgrade to occur.

16 At the IPL> prompt, verify the i2004 and i2002 Internet Telephones are upgraded for each Voice Gateway Media Card by entering the following:

isetShow

Inspect the list to ensure all i2004 and i2002 Internet Telephones have the correct firmware version.

17 For any i2002/i2004 Internet Telephones that did not upgrade successfully, try one of the following (in order):

- Use the **isetReset "IP Address"** command.
- Enter the following combination of key strokes at the telephone console: **release**, **mute**, **up**, **down**, **up**, **down**, **up**, **mute**, **9**, **release**.
- Power the telephone off and then on again.

If the upgrade was unsuccessful on any of the i2004.i2002 Internet Telephones, this is most likely due to one of the following:

- one of the Voice Gateway Media Cards did not upgrade the software successfully
- an i2002/i2004 Internet Telephone is loaded with a firmware version that was unable to be upgraded by the Voice Gateway Media Card in the normal way
- the umsUpgradeAll command has not been issued
- one of the cards may not have been reset

If the upgrade was unsuccessful, re-do the appropriate procedure. If the upgrade is still unsuccessful, contact your technical support representative for further assistance.

End of Procedure

For additional information on configuring the i2002 and i2004 Internet Telephones and the i2050 Software Phone, see *Internet Terminals Description* (553-3001-217).

Upgrading the Voice Gateway Media Card firmware

The minimum versions of the card firmware for the Voice Gateway Media Card are:

- Version 6.4 for the Succession Media Card
- Version 5.6 for the ITG-P Line Card

To upgrade the card firmware, follow the steps in Procedure 53 on page 401.

Procedure 53
Upgrading the Voice Gateway Media Card firmware

1 Check the Nortel Networks Web site for the most current versions of the firmware for the ITG-P Line Card and Succession Media Card. To download firmware files from Nortel Networks, follow the steps in Procedure 111 on page 719.

2 Once the most current version of the firmware has been downloaded, follow the steps in:

- Procedure 90 on page 590 to upgrade the firmware on the ITG-P Line Card
- Procedure 91 on page 592 to upgrade the firmware on the Succession Media Card

End of Procedure

Configure OTM alarm management to receive IP Line SNMP traps

Alarm management cannot be configured using Element Management. OTM must be used to configure the alarm management feature to receive IP Line SNMP traps. See Procedure 31 on page 323.

Assemble and install an Internet Telephone

To assemble and install an Internet Telephone, refer to the *Internet Terminals Description* (553-3001-217).

Change the default IPL> CLI Shell password

The IPL> Command Line Interface (CLI) is password protected for Telnet access and access to the local maintenance port. The same user name and password also protects FTP access to the Voice Gateway Media Card. The IPL> CLI has a default user name of itgadmin and a default password of itgadmin.

The default user name and password must be changed as a preventative security measure. See "Changing the IPL> CLI Shell user name and password" on page 411 and Procedure 55 on page 415.

Configure the Internet Telephone Installer Passwords

The Internet Telephone Installer Password protection, for changing the TN on the telephone, controls registration with a virtual line TN on the Call Server. Refer to page 420 for more information about the Internet Telephone Installer Passwords.

To enable and set the administrative Internet Telephone Installer Password, see Procedure 58 on page 429. If needed, enable and set a temporary Internet Telephone Installer Password. See Procedure 59 on page 433.

> ***Note:*** Configuring the Internet Telephone Installer Passwords can be done using the CLI. However, Element Management can be used to configure the Internet Telephone Installer Passwords for a Succession CSE 1000 Rel 2.0 system (see "Setting the Internet Telephone Installer Password" on page 545).

Importing node configuration from an existing node

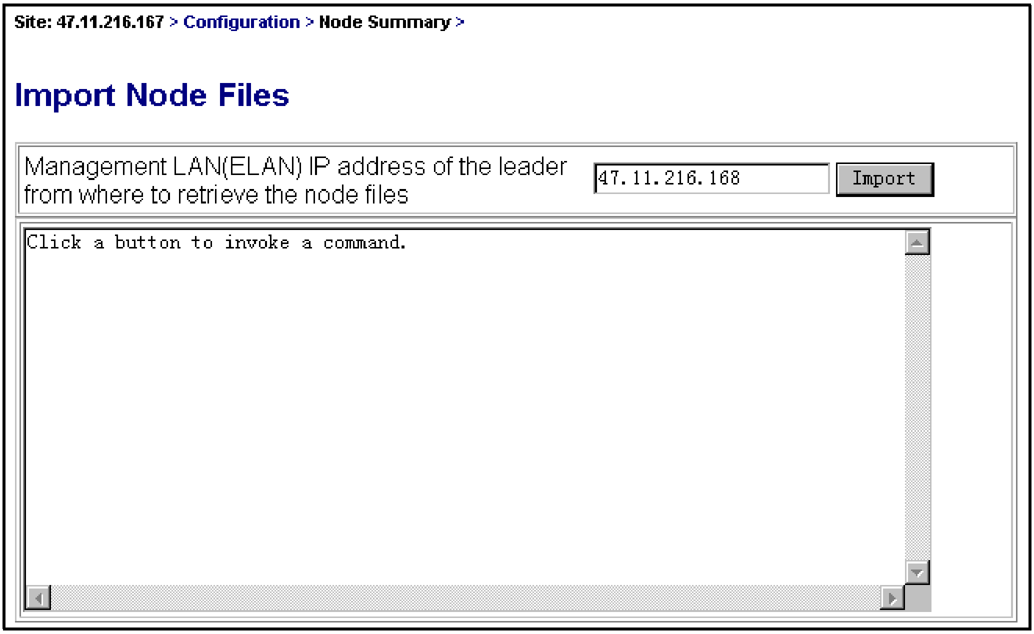
It is possible to import a node and its configuration data from an existing node into Element Management.

For example, if Node 151 exists but does not exist on the Call Server, then Node 151 can be imported into Element Management. Once imported, the node configuration data can be updated and edited.

Procedure 54
Importing node files

1. In the Navigation Tree, click **Configuration** and then **IP Telephony**.
2. The Node Summary page appears. Click the **Import Node Files** button. The Import Node Files page appears (see "Import node files" on page 404).

Figure 97
Import node files

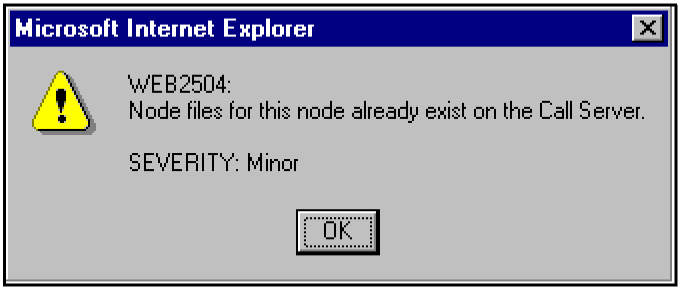


3 Enter the Management LAN (ELAN) IP Address of the Leader in the text box. This address is used to retrieve the node files.

4 Click the **Import** button.

If the node already exists on the Call Server, a message appears indicating that the node already exists on the Call Server (see Figure 98 on page 405).

Figure 98
Duplicate node information

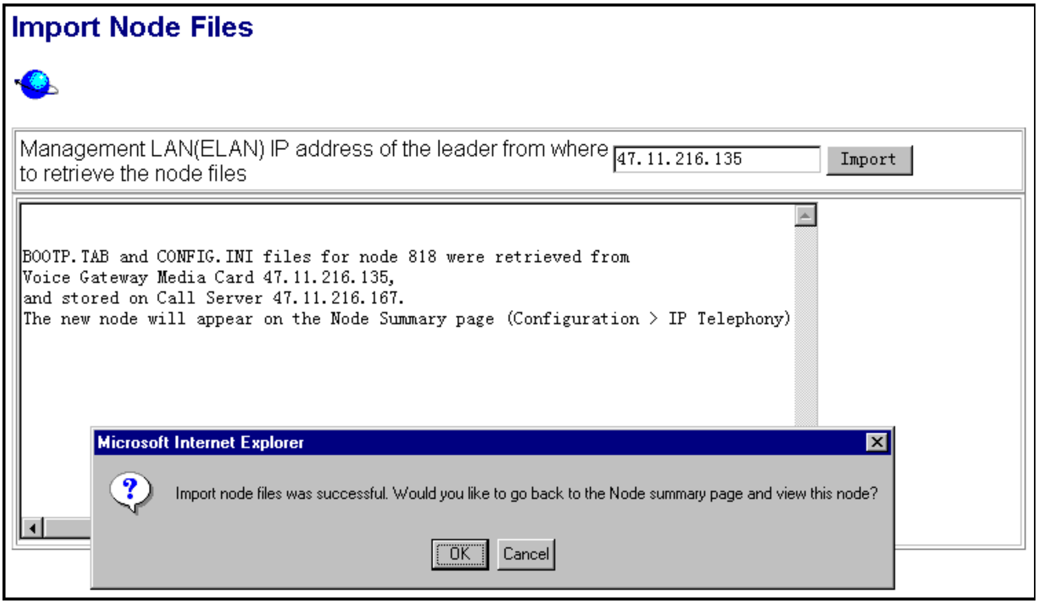


If the node does not exist, Element Management tries to write the configuration to the Call Server. If it succeeds, a message indicating the import was successful appears (see Figure 99 on page 406). If Element Management cannot write the configuration to the Call server, a fail reason appears in the text area of the Import Node Files page.

5 If the import is successful, information appears in the text area of the Node Import Files screen (see Figure 99 on page 406) and a message box also appears. In the message box, click the **OK** button to proceed to the **Node Summary** page. The node information can then be viewed and edited if necessary.

If node import is unsuccessful, an error message appears in text box area.

Figure 99
Import Node Files–Successfully imported node



End of Procedure

IP Line Application Administration

Contents

This section contains information on the following topics:

Reference list

The following are references for this section:

- *Features and Services* (553-3001-306)
- *Software Input/Output: Administration* (553-3001-311)

Overview

This chapter explains how to administer IP Line 3.0 and the Voice Gateway Media Cards on the Meridian 1 and Succession Communication Server for Enterprise 1000 systems.

Administration procedures include activities such as monitoring system status, operational reports, performing upgrades, changing configuration, adding, changing, and removing cards. Administration does not include engineering, provisioning, initial installation and configuration, maintenance, or troubleshooting.

The Voice Gateway Media Card provides four administration interfaces:

- Optivity Telephony Manager (OTM) 2.0

  OTM's IP Line application provides a graphical user interface to the Voice Gateway Media Card. OTM is used to Telnet to the card, install and upgrade loadware and firmware, configure alarm event reporting, view and update card property and configuration data, add new cards to a node, schedule reports and other related tasks. OTM is the primary interface for Meridian 1 and Succession Communication Server for Enterprise (CSE) 1000 Rel 1.1 systems.

- Succession CSE 1000 Element Management

  Element Management is a Web server that provides a graphical user interface using a Web browser. Element Management is used to telnet to the card, install and upgrade loadware and firmware, configure alarm event reporting, view and update card property and configuration data, add new cards to a node, schedule reports and other related tasks. The Element Management Web server interface is used for administration of Succession CSE 1000 Rel 2.0 systems.

- IPL> Command Line Interface (CLI)

  Use the CLI to display card and node status, change passwords, check software versions, view channel states, and other card information. The CLI is also used for expert level support and debug. The prompt for the CLI on the Voice Gateway Media Card is IPL>. Access the CLI through a direct serial connection to the I/O panel serial port, the Maint Port on the faceplate, or through a Telnet session. Use a VT-100 terminal emulation program set to 9600 baud, 8 bits, no parity, one stop bit.

- Meridian 1 and Succession CSE 1000 Overlays

  Use the same commands and messages for the Voice Gateway Media Card as you would for any other Line card.

Password Security

There are password security features that must be configured and administered in IP Line 3.0. The password security features are:

1 SNMP Community Name Password

2 IPL> CLI Shell Password
(for Meridian 1 and CSE 1000 Rel 1.1 systems)

3 Call Server's Level 1 Password (PWD1)
(for Succession CSE 1000 Rel 2.0 systems)

4 Internet Telephone Installer Password

The Internet Telephone Installer Password works at the node level. While, the SNMP Community Name password, IPL> CLI Shell password, and Call Server's Level 1 Password operate at the card level.

- The Internet Telephone Installer Password is first applied to one card in the node, and then is applied to all the cards in the node.
- The SNMP Community Name password is contained in the card properties that were transmitted to each card.
- The IPL> CLI Shell password is set on each individual card.
- The Level 1 Password is set at the Call Server and is sent to all cards in the node.

SNMP Community Names password

SNMP Community Names passwords are required to access the Voice Gateway Media Card. There are two community names, Current and Previous.

OTM stores both community names (see Figure 45 on page 295) for Meridian 1 and Succession CSE 1000 Rel 1.1 systems. The Previous community name is used to access the Voice Gateway Media Card when changing the community name. Procedure 21 on page 295 explains how to change the SNMP community names to provide greater security for the IP Telephony node.

Element Management stores the community names (see Figure 63 on page 344) for Succession CSE 1000 Rel 2.0 systems. Procedure 35 on page 344 is used to change the SNMP community name to provide increased security.

Changing the IPL> CLI Shell user name and password

The IPL> Command Line Interface (CLI) is password protected for Telnet access and access to the local maintenance port. The same user name and password also protects FTP access to the Voice Gateway Media Cards.

Login Banner Enhancement

The IP Line 3.0 login banner for the Voice Gateway Media Cards has been enhanced to include the ITG Trunk 2.0 application's login banner information. This information is helpful when logging into a card at a site as critical information identifying the card is displayed. The information includes the card loadware version, ELAN IP address, card type, firmware version, current time and date, system name, system location, and system contact.

The following information is an example of the login banner displayed on the Succession Media Card:

Login:
Password

Welcome to the IP Line command line.
Software Version: IPL-3.00.36
Management IP: 47.11.216.216
Host Type: Succession Media Card
Firmware Version: ITG Firmware Rls 4.0

SysName: ITG Line
SysLocation: TN 10 0
SysContact: designer

OS Time: Date (04/03/2002) Time (09:07:43)
Use "logout" to logout.
Idle session timeout = 20 minutes.
IPL>

Password Guessing Protection

Protection against password guessing has been implemented in IP Line 3.0. This blocks a hacker from attempting to log into the ITG-P Line Card or Succession Media Card shell by continuously guessing the shell user name and password. The password guessing protection is applicable to either a tip session (direct maintenance port connected TTY session) or a Telnet session.

The password guessing protection feature is described as follows:

- There is a login failure threshold of 3 and a lockout period of 10 minutes. This is not user configurable.
- Password guessing protection is enabled by default when the card starts the first time. The protection can be disabled and re-enabled at the VxWorks shell. Entering the **shellLoginProtectSet 0** command disables the protection and **shellLoginProtectSet 1** enables it.

- When the login failure threshold is exceeded (by 3 consecutive failed login attempts), the system raises an "ITG1038" critical alarm. This alarm is sent to indicate the card's login has been locked due to too many incorrect password entries.

  Alarm value = ITG alarm 38
  perceivedSeverity = Critical
  probableCause = Unauthorized maximum access attempts
  Alarm text = IPL login protection (login locked)

  When the 10 minute timer expires for the lockout period, the system raises an "ITG5038" cleared alarm. The clear message is sent after the lockout period expires.

  perceivedSeverity = Cleared
  probableCause = Unauthorized maximum access attempts
  Alarm text = IPL login protection (login available)

- There is no online indication or warning during the failed login attempt lockout state. Everything appears the same to the user trying to login. The user is not informed that login blocking has been activated, the login is ignored for 10 minutes.

  Note: Both the "critical" and "cleared" alarms send an SNMP trap to the system administrator. For security reasons, these two alarms do not call the syslog function as the other itgAlarms do, so no syslog message is displayed on the console or written in the syslog file.

- On the Voice Gateway Media Card, the faceplate displays GO38 (ITG1038) when the ITG1038 alarm is received since it is a critical alarm. The ITG5038 clears GO38 from the faceplate when the 10 minute timer expires.

The default user name and password

The IPL> CLI has a default user name of **itgadmin** and a default password of **itgadmin**. The default user name and password must be changed as a preventative security measure. The shellPasswordSet command changes the IP Line username and password.

> **WARNING**
>
> Do not leave the IPL> CLI shell user name and password as the default.
>
> Implement a good security policy where the user name and password are changed periodically.

The first step to protect the security of the IPL> CLI is to change the default user name and password (see Procedure 55 on page 415).

To maintain a proper level of security, frequently change the user name and password (see Procedure 56 on page 416).

If the user name or password is forgotten or has to be reset to the default, follow the steps in Procedure 57 on page 417.

Changing the default IPL> CLI shell user name and password

To change the default user name and password of the IPL> Command Line Interface, follow the steps in Procedure 55 on page 415.

Procedure 55
Changing the default IPL> CLI shell user name and password

1 From the IPL> CLI, use the command **shellPasswordSet** to change the default user name and password.

The default user name is **itgadmin** and the default password is **itgadmin**.

2 The prompts appear as follows:

Enter current user name: itgadmin
Enter current password: itgadmin
Enter new user name: newname
Enter new password: newpwd
Enter new password again to confirm: newpwd

Note: The new password must be 8 to 12 characters. You should not re-use the default user name and password.

3 If the entire sequence of commands is successfully entered, the system response is 'value = 0 = 0x0'. The new user name and password are now stored in non-volatile RAM on the Voice Gateway Media Card, and are retained even if the card is reset, powered-off, or powered-on.

End of Procedure

Changing the current user name and password

Good security policy requires changing user names and passwords periodically. To change the IPL> user name and password after it has been changed from the defaults, follow the steps in Procedure 56 on page 416.

Procedure 56
Changing the current IPL> CLI Shell user name and password

It is good practice to change the IPL> CLI Shell user name and password periodically. Never leave the user name and password as their defaults.

1 From the IPL> CLI, use the command **shellPasswordSet** to change the current IPL> CLI shell user name and password.

2 The prompts are displayed as follows:

Enter current user name: currentname
Enter current password: currentpwd
Enter new user name: <newname>
Enter new password: <newpwd>
Enter new password again to confirm: <newpwd>

Note: The new password must be 8 to 12 characters. You should not re-use the default user name and password.

3 If the entire sequence of commands is successfully entered, the system response is 'value = 0 = 0x0'. The newly set user name and password are now stored in non-volatile RAM (NVRAM) on the Voice Gateway Media Card. They are retained even if the card is reset, powered-off, or powered-on.

End of Procedure

Resetting the IPL> CLI Shell user name and password

If the authorized system management personnel do not have the current IPL> CLI Shell user name and password, reset the user name and password to default (itgadmin and itgadmin).

To reset the IPL> CLI shell user name and password, follow the steps in Procedure 57 on page 417. This procedure requires a connection to the local maintenance port on the Voice Gateway Media Card and also requires rebooting the card which will interrupt services.

Procedure 57
Resetting the user name and password to default

1. Connect a terminal to the Maintenance port (labeled Maint) either directly or through a dial-up modem. The terminal communication parameter must be 9600bp, 8 data bits, no parity, and 1 stop bit.
2. Press the **Enter** key on the keyboard. The **IPL>** prompt is displayed.
3. Reboot the card by pressing the **RESET** button on the faceplate of the card with a pointed object, such as a ball-point pen.

> **WARNING**
> Do not use a pencil to reset the Voice Gateway Media Card. The graphite carbon can create an electrical short circuit on the board.

4. Start up messages are displayed on the terminal. Type **jkl** on the terminal keyboard when you see the prompt.

   Note: jkl runs from bios or boot ROM which is printed early in the bootup process. There is only a six second window at the prompt to enter jkl. If you miss the prompt, restart the card and repeat the above step.

5. Once the card has booted from bios or boot ROM, a CLI prompt such as the BIOS> appears. Enter the following command **shellPasswordNvramClear** at the prompt.
6. Type **reboot** at the prompt to reboot the card.
7. Wait for the card to completely reboot into the IP Line application.
8. Login using the default user name (**itgadmin**) and password (**itgadmin**).

9 Perform Procedure 56 on page 416 to change the IPL> CLI user name and password.

Note: Never leave the default user name and password on a system that is in service. An effective security policy requires frequent change of the IPL> CLI user name and password.

End of Procedure

Node Password synchronization

The Succession CSE 1000 Rel 2.0 system requires the BOOTP.TAB, CONFIG.INI, and Internet Telephone firmware files to be the same on all cards in the system. The cards that can be in the system are the ITG-P Line Card, Succession Media Card, and the Signaling Server. To keep consistent configuration within the system, files are transferred from the Leader to the Follower cards using FTP.

In the Succession CSE 1000 Rel 2.0 system, the same userid and password is used for Telnet access to the CLI of the Voice Gateway Media Card and for the FTP process. In order for the FTP process to work correctly, all the cards in a node must be synchronized with the same userid and password. To ensure node password synchronization (all the cards have the same userid and password), all cards use the Call Server's Level 1 Password (PWD1) userid and password.

A card uses its userid and password when it tries to access another card to FTP files. The FTP fails unless all the cards have the same userid and password. The FTP fails because of failed user authentication. Therefore, a unique userid and password should be used within one Succession CSE 1000 Rel 2.0 system.

Since most applications (except the Gatekeeper) communicate directly with the Call Server, the Call Server's Level 1 PWD1 userid and password is the unique password among all platforms.

Level 1 Password (PWD1)

The minimum password length on the Call Server is four characters. However, the minimum password on the Succession Media Card and the Signaling Server is eight characters. To make the passwords match, the PWD1 is padded at the end with spaces if the password is less than eight characters.

For example, if the Call Server's PWD1 is "0000", it is padded to the right with the four space characters to become "0000   ". A user logging in to the CLI of any Voice Gateway Media Card or Signaling Server must enter four zeros followed by four spaces.

Password Updates

The PWD1 userid and password is sent to all cards when:

- the cards initially establish a connection with the Call Server across the ELAN
- an EDD operation that is performed on the Call Server

Once the PWD1 information is downloaded, it is saved in the card's NVRAM. If a card has not established a link with the ELAN, the userid and password that is currently stored in the card's NVRAM is used to login. The userid and password may not match the PWD1 on the Call Server because the Call Server has not yet downloaded the current PWD1 to the card. Once the ELAN connection is established, the userid and password are synchronized on all cards. The userid and password in the card's NVRAM is overwritten with the new userid and password from the Call Server.

Since all cards automatically receive the userid and password from the Call Server, the password can be changed in a single location, the Call Server's CLI. This eliminates the need to change the password on every card in the node (just change the password once on the Call Server). When the password is changed at the Call Server, the password is automatically sent to all the Voice Gateway Media Cards.

A user can change the userid and password login on any card using the shellPasswordSet CLI command. However, updates from the Call Server overwrite the cards userid and password in the NVRAM.

If the PWD1 is changed and an EDD operation is not performed, the cards can contain a mixture of old and new passwords. This could happen if a new card is plugged in, an existing card reboots or loses and reestablishes its ELAN connection. Nortel Networks recommends that an EED be performed when the PWD1 password is changed on the Call Server. This ensures that all cards have the new PWD1 userid and password.

For more information on the PWD1 Level 1 password, see the “LD 17 Gate OpenerPWD (Password)” section in the *Software Input/Output: Administration* (553-3001-311).

Internet Telephone Installer Password

An Internet Telephone displays Node ID and Terminal Number (TN) of the telephone for five seconds as the telephone boots up. ITG Line 2.2 introduced the availability of password protection for changing the TN on the Internet Telephone. This feature is available on the i2002 and i2004 Internet Telephones and i2050 Software Phone. The Internet Telephone Installer Password protection, for changing the TN on the telephone, controls registration with a virtual line TN on the Call Server.

> ***Note:*** For Succession CSE 1000 Rel 2.0 systems, the Internet Telephone Installer Password can also set using the CLI commands in Element Management.

Administrator Internet Telephone Installer Password

This feature adds basic Internet Telephone Installer Password protection on the Internet Telephones to control registration with a virtual line TN on the Call Server. This feature does not provide a user password nor a Station Control Password for Internet Telephones.

i2004 Internet Telephone

When the password is configured, the i2004 Internet Telephone screen shows:

1 The four digit Node ID and a Password prompt (see Page 1 of Figure 102 on page 425), instead of the Node ID and TN fields (see Figure 100 on page 423).

2 When the user enters the password, an asterisk (*) is displayed for each digit entered. The password is not shown.

3 Once the Node ID and Password are entered, the user presses OK. If the password passes the Connect Server's authentication, a screen is displayed with the TN field (see Figure 102 on page 425).

i2002 Internet Telephone

When the password is configured, the i2002 Internet Telephone screen shows:

1 The four digit Node ID screen is displayed first (see Figure 103 on page 426).

2 The user is then prompted with the Password screen (see Figure 103 on page 426) instead of the TN field screen (see Figure 101 on page 423).

3 When the user enters the password, an asterisk (*) is displayed for each digit entered. The password is not shown.

4 Once the Password is entered, the user presses OK. If the password passes the Connect Server's authentication, a screen is displayed with the TN field (see Figure 103 on page 426).

If the Node ID and Password are not entered, the registration continues after five seconds and the TN is not displayed. If an invalid Node ID password is entered, the Node ID and Password screen is redisplayed. This screen is redisplayed a maximum of two times, giving the technician a total of three chances to enter the password. After three failed attempts, the registration continues as if there were no password entries. The technician can reboot the telephone and try again if more tries are needed.

If the technician has entered a zero length (null) password, then the Node ID, TN, and Password screens are not displayed on the Internet Telephone during the registration process. This provides the most security as it prevents any entry of passwords or TNs from the Internet Telephone.

Temporary Internet Telephone Installer Password

A Temporary Internet Telephone Installer Password can be configured, which enables the technician to give temporary user access to the TN for configuration. A temporary password removes the need to distribute the Node password and having to change it afterwards. The temporary password is automatically deleted after it has been used to the defined number of times or when the duration expires, whichever comes first.

The following are examples of situations where the Temporary Internet Telephone Installer Password can be used:

- A department is installing i2050 Software Phones. The technician creates a temporary password, sets an appropriate number of uses (such as allowing two logins for each telephone in case there is a problem the first time) and sets the duration to expire by the end of the weekend. The password access automatically ends before Monday morning (or sooner if the number of uses expires).
- A telecommuter needs to install an Internet Telephone. The technician provides the temporary password, that expires the next day or after two uses. When the Internet Telephone Installer Password protection is enabled, the Set TN is not displayed as part of the Set Info sub menu of the Telephone Option menu. The telephone's TN can be retrieved on the core CPU through the LD 20 PRT DNB and LD 32 IDU, or LD 80 TRAC, or PDT> rlmShow. It can also be found on the Voice Gateway Media Card through IPL> isetShowByIP.

Registration screens with TN password feature

The following screens shows the existing TN entry screen that appears when the Internet Telephone registers:

- Figure 100 on page 423 displays the screen on the i2004 if password protection is disabled or not configured.
- Figure 101 on page 423 displays the screen on the i2002 if password protection is disabled or not configured.

Figure 100
i2004 registration with no password checking

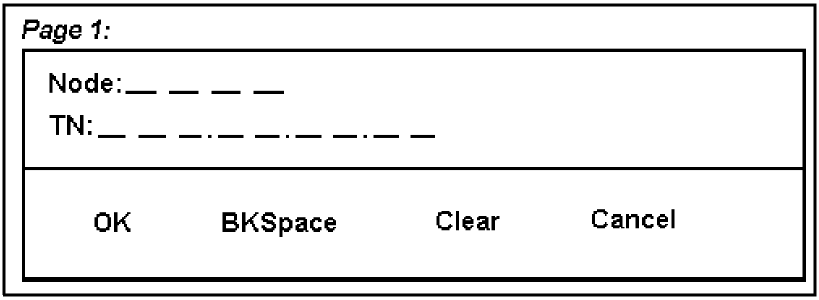
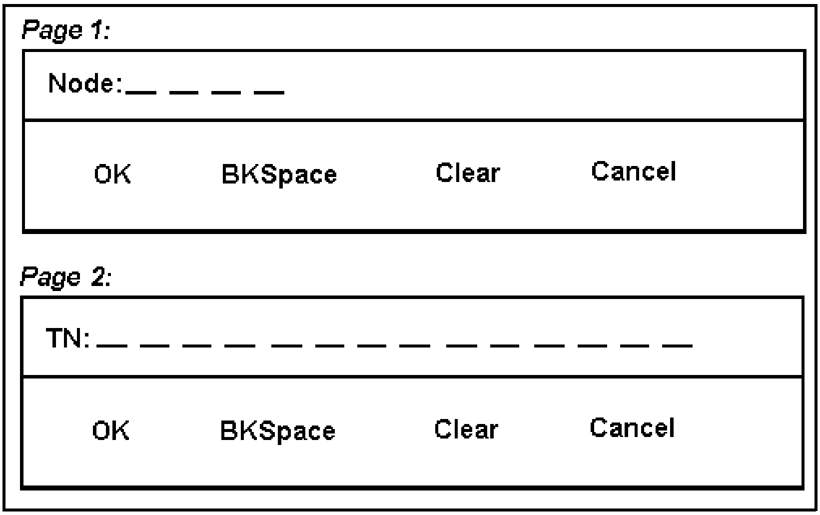


Figure 101
i2002 registration with no password checking



When the TN password protection feature is configured with a non-zero length password and is enabled:

- Figure 102 on page 425 shows the i2004 TN entry screens.
  - — Figure 102 on page 425 displays the Node ID and Password. Note the Password entry input field is blank (underscores are not displayed). Therefore, the maximum length of the password is not disclosed.
  - — If the correct password is entered, the TN is displayed (see Figure 102 on page 425).
- Figure 103 on page 426 shows the i2002 TN entry screens.
  - — Figure 103 on page 426 displays the Node ID. The Node ID is entered and the user presses OK.
  - — Figure 103 displays Password entry page. Note the Password entry input field is blank (underscores are not displayed). Therefore, the maximum length of the password is not disclosed.
  - — If the correct password is entered, the TN (Figure 103) is displayed.

Figure 102
i2004 registration with password checking

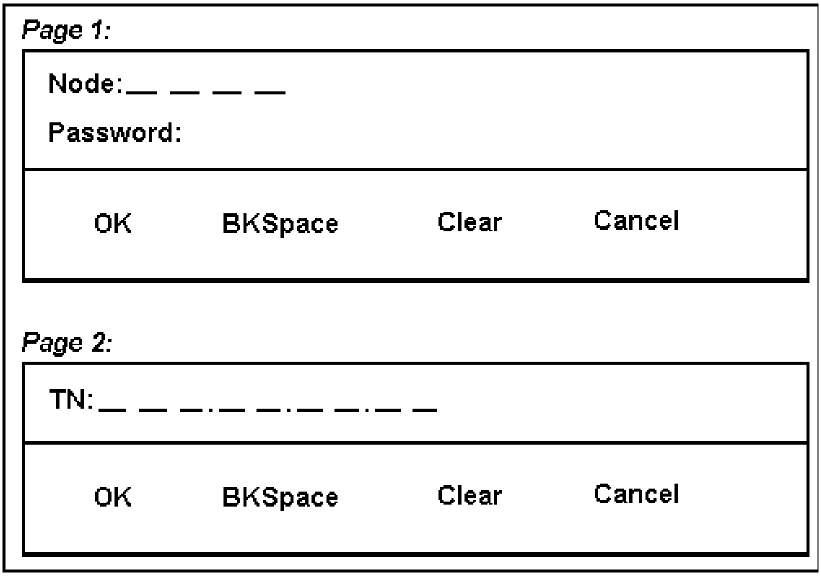
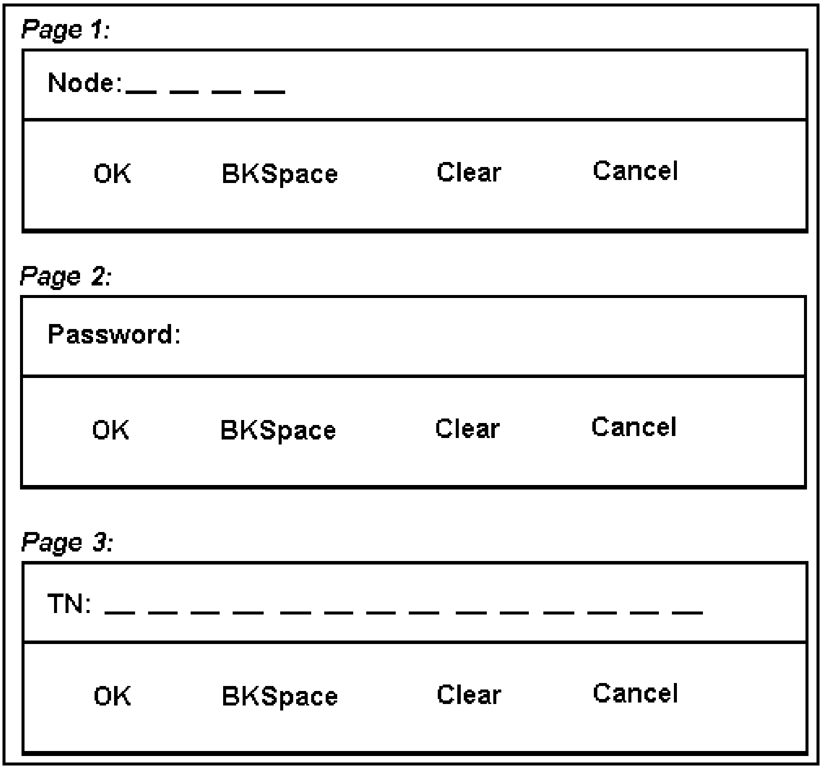


Figure 103
i2002 registration with password checking



IP Line CLI commands for password control

The Internet Telephone Installer Passwords are configured on any Voice Gateway Media Card in the node. The Internet Telephone Installer Password is configured and administered using a set of six IPL> CLI commands:

- nodePwdSet "password"
- nodePwdShow
- nodePwdTempPwdSet "temppwd", uses, <time>
- nodeTempPwdClear
- nodePwdEnable
- nodePwdDisable

The commands begin with "node" as they work at the node level. For detailed information about these commands, see Table 83 on page 578.

When an IP Telephony node is first installed, the Internet Telephone Installer Password is not defined or enabled by default. To prevent users from inadvertently reconfiguring the Node ID and TN on their Internet Telephones, enable the Internet Telephone Installer Password after the Internet Telephone is initially installed and the system is in service.

Password security prevents casual access to an Internet Telephone's TN for the purpose of registering to a different virtual line TN on the Meridian 1 and Succession CSE 1000 Call Server after the Internet Telephones have been installed. A password is not encrypted by the telephone or the Voice Gateway Media Card.

By default, when a node is initially installed, the administrative password and the temporary password are not defined. The password feature is also in the disabled state.

The **nodePwdSet "password"** command sets and enables the password. When the password is enabled and configured, the screen on the Internet Telephone displays the four digit Node ID and a Password prompt, instead of the Node ID and TN fields.

> **WARNING**
>
> The nodePwdSet command with no "password" parameter enables the administrator password and sets a null (zero-length) password.
>
> Enabling the administrator password and setting a null password makes it impossible to install the Internet Telephones because the Node ID and TN prompts are not displayed on the telephone screen.
>
> Always specify the "password" parameter when issuing the nodePwdSet command. This password parameter is 6-14 digits. The valid characters are 0-9 * #.

If the **nodePwdEnable** command is entered before the password is set using the nodePwdSet command, the password is also enabled with a null password and as a result, the password and TN prompts are also never displayed on the Internet Telephones.

The administrator normally uses the administrative Internet Telephone Installer Password if it is necessary to install a new telephone or change the configuration (Node ID and TN) of an existing telephone.

> ***Note:*** If you are unable to install an Internet Telephone because you are not prompted for a Node ID and TN, login to a Voice Gateway Media Card and check the status of the password using the **nodePwdShow** command.

The administrator can create a temporary Internet Telephone Installer Password for experienced users who are delegated to install Internet Telephones. If a null administrator password is set and a temporary password is created, the temporary password overrides the null administrator password.

If the administrator wishes to suppress all password prompting to reconfigure the Node ID and TN, then the temporary password should be cleared using the **nodeTempPwdClear** command. Also, set the administrative password to a null password using the **nodePwdSet** command with no "password" parameter specified.

Setting the Internet Telephone Installer Passwords

The Internet Telephone Installer Passwords are configured on one Voice Gateway Media Card or on the Signaling Server in the node. The passwords are then applied to all cards in the node.

Administrative Internet Telephone Installer Password

The administrative Internet Telephone Installer Password is used by the administrator to install a new telephone or change the configuration (Node ID and TN) of an existing telephone.

To set the administrative Internet Telephone Installer Password, see Procedure 58 on page 429.

Procedure 58
Configuring the administrative Internet Telephone Installer Password

1 Connect to any Voice Gateway Media Card in the node.

2 Login to the IPL> CLI and type the **nodePwdShow** command. This command displays the settings of the Internet Telephone Installer (node) password.

If in the default state, the Internet Telephone Installer Password has never been set. The nodePwdShow command should display the following:

```
NodeID    PwdEna    Pwd        TmpPwd     Uses      Timeout
======    =======   ========   ========   =======   ===========
123       No                                        0d 0h 0m 0s
```

where:

NodeID–the Internet Telephone Installer Password configuration applies to all Voice Gateway Media Cards on the same TLAN that belong to this Node ID.

PwdEna–by default the cards should be in disabled state (PwdEna=No). The PwdEna setting specifies the enabled (Yes) or disabled (No) state of the Internet Telephone Installer Password.

Pwd–this is the administrator Internet Telephone Installer Password. In the default state, the administrator password is null.

TmpPwd–this is the temporary Internet Telephone Installer Password. In the default state, the temporary password is null.

Uses–the Uses parameter applies to the temporary Internet Telephone Installer Password. In the default state, this setting is null. If the card is not in the default state, the Uses parameter is a numeric value from 0-1000. This number specifies the remaining number of uses for the temporary password. If zero is entered for the Uses parameter when setting the temporary password, the Time parameter is mandatory. As a result, the password expires based on time instead of a number of uses.

Timeout–the Timeout heading corresponds to the Time parameter of the temporary Internet Telephone Installer Password. In the default state the Time is null. If the card is not in the default state, this setting specifies the duration in hours in which the temporary password is valid. The range is 0-240 hours (which is a maximum of 10 days). The number specified under Timeout indicates the remaining time to expire of the temporary password. The Time parameter is optional if the Uses parameter is non-zero and it is mandatory if the Uses parameter is set to zero.

Note: If both the Uses and Time parameters are entered, the password expires on whichever comes first. That is, Uses is reduced to zero or the Time has expired. If both the Uses and Time parameters are entered and are set to zero, it is the same as not setting the temporary password.

Next set the administrator Internet Telephone Installer Password. The **nodePwdSet "password"** commands enables and sets the administrator password. The "password" parameter can be null, or 6 to 14 digits in length. The valid characters are 0-9 * #. This command can be entered at any time. The new password entered simply overwrites the previous password.

Set the administrator password, first with a null password and then with a password specified.

3 Type **nodePwdSet** at the IPL> prompt. Note no password parameter is specified.

Type **nodePwdShow** to see the following:

NodeID	PwdEna	Pwd	TmpPwd	Uses	Timeout
======	=======	========	========	=======	===========
123	Yes				0d 0h 0m 0s

PwdEna–the administrator password is now enabled (PwdEna=Yes).

Pwd–with no "password" parameter specified the administrator password is null. Internet Telephones cannot be installed when the password is null. A null password causes the Node ID and Password screen to be skipped during restart.

WARNING

The nodePwdSet, with no parameter, by default enables the administrator password and sets a null (zero-length) password.

Internet Telephones cannot be installed if the administrator password is enabled and set to null.

Always specify the password parameter to install Internet Telephones.

4 Type **nodePwdSet "password"** at the IPL> prompt, where the password parameter is 6 to 14 digits in length. The valid character are 0-9 * #. For this example, use "1234567" as the password.

5 Type **nodePwdShow** to see the following:

```
NodeID   PwdEna    Pwd        TmpPwd     Uses      Timeout
======   =======   ========   ========   =======   ===========
123      Yes       1234567                         0d 0h 0m 0s
```

PwdEna–the administrator password is enabled (PwdEna=Yes).

Pwd–the administrator password, 1234567, is displayed.

Note: Always specify the "password" parameter when entering the nodePwdSet command.

6 The **nodePwdEnable** and **nodePwdDisable** commands enable and disable the administrative Internet Telephone Installer Password, respectively.

End of Procedure

Temporary Internet Telephone Installer Password

A temporary Internet Telephone Installer Password can be set. This enables temporary user access to the TN for configuration. A temporary password removes the need to distribute the administrative (node) password and then the need to change it afterwards. If there is a null administrator password set and you create a temporary password, the temporary password overrides the null administrative password.

The syntax for temporary Internet Telephone Installer Password specifies the password, the number of times that the password can be entered, and the time that the password is valid.

To set a temporary Internet Telephone Installer Password, see Procedure 59 on page 433.

Procedure 59
Configuring the temporary Internet Telephone Installer Password

1 Type **nodeTempPwdSet "password", uses, <time>** at the IPL> prompt, where "password" is the temporary password string 6 to 14 digits in length, uses is the value from 0 to 1000, and time is between 0 and 240 hours.

For example, nodeTempPwdSet "987654", 15, 3

2 Type **nodePwdShow** to see the following:

```
NodeID   PwdEna    Pwd        TmpPwd     Uses      Timeout
======   =======   ========   ========   =======   ===========
123      Yes       1234567    987654     15        0d 3h 0m 0s
```

3 The temporary password is automatically deleted after it has been used the defined number of times (Uses) or when the duration expires (Timeout), whichever comes first. However, to delete the temporary password before the number of uses or time has expired, type **nodeTempPwdClear** command at the IPL> prompt.

4 Type **nodePwdShow** to ensure the temporary password has been deleted.:

```
NodeID   PwdEna    Pwd        TmpPwd     Uses      Timeout
======   =======   ========   ========   =======   ===========
123      Yes       1234567                         0d 0h 0m 0s
```

End of Procedure

Reset the Operational Measurements

Reset the Operational Measurements (OM) file if incorrect statistics may have been collected.

At the IPL> prompt, type: **resetOM**.

The resetOM command resets all operational measurement parameters that have been collected since the last log dump. The statistics start from zero.

Display the number of DSPs

The DSPNumShow command displays the number of DSPs on the Voice Gateway Media Card.

At the IPL> prompt, type: **DSPNumShow**.

Display IP Telephony node Properties

The IPInfoShow command displays information about an IP Telephony node.

At the IPL> prompt, type: **IPInfoShow**

The following IP Telephony node information is displayed on the TTY:

- IP addresses for the management and voice subnets
- default router for the management and voice subnets
- subnet mask for the management and voice subnets
- SNMP manager
- IP routing table
- IP configuration of the card (which is related to the IP configuration of the node)

The IPInfoShow command displays information similar to the following:

Maintenance Interface = lnIsa0
Maintenance IP address = 47.103.220.199
Maintenance subnet mask = 255.255.255.224
Voice Interface = lnPci1
Voice IP address = 47.103.247.221
Voice subnet mask = 255.255.255.0

ROUTE NET TABLE

destination	gateway	flags	Refcnt	Use	Interface
0.0.0.0	47.103.247.1	3	7	5800883	lnPci1
47.103.220.192	47.103.220.199	101	0	0	lnIsa0
47.103.247.0	47.103.247.221	101	0	0	lnPci1
47.103.247.0	47.103.247.221	101	0	0	lnPci1

ROUTE HOST TABLE

destination	gateway	flags	Refcnt	Use	Interface
127.0.0.1	127.0.0.1	5	0	0	lo0

value = 77 = 0x4d = 'M'

Display Voice Gateway Media Card properties

The itgCardShow command displays information about a Voice Gateway Media Card. At the IPL> prompt, type: **itgCardShow**

The itgCardShow command displays information similar to the following:

Index : 1
Type : EXUT
Role : Leader
Node : 123
Leader IP : 47.103.247.220
Card IP : 47.103.247.221
Card TN : 44 0 10
Card State : ENBL
Uptime : 1 days, 19 hours, 43 mins, 11 secs (157391 secs)
Codecs : G711Ulaw(default), G711Alaw, G729AB
lnPci stat : 100 Mbps (Carrier OK)
value = 1 = 0x1

The following commands provide additional information about a Voice Gateway Media Card:

- ifShow
- serialNumShow
- firmwareVersionShow
- swVersionShow

Transfer files using the Command Line Interface

There are a number of special file transfer commands available to Put/Get files from the IPL> CLI. These commands are normally used as part of an expert support procedure if OTM or Element Management are not available.

These commands (see Table 64 on page 437) are from the perspective of the Voice Gateway Media Card. If “Get” is part of the command, the file transfers from the OTM PC to the Voice Gateway Media Card. If “Put” is part of the command, the file transfers from the Voice Gateway Media Card to the OTM PC.

To transfer a file, enter one of the commands in Table 64 on page 437 at the IPL> CLI depending on what type of file transfer is to occur.

The following commands can be entered at the IPL> CLI:

Table 64
IPL> CLI Commands–File Transfer

Command	Parameters
swDownload	<hostname> <username> <password> <directory path> <filename>
configFileGet	<hostname> <username> <password> <directory path> <filename>
bootPFileGet	<hostname> <username> <password> <directory path> <filename>
hostFileGet	<hostname> <username> <password> <directory path> <filename> <ITGFileName> <listener>
bootPFilePut	<hostname> <username> <password> <directory path> <filename>
currOMFilePut	<hostname> <username> <password> <directory path> <filename>
prevOMFilePut	<hostname> <username> <password> <directory path> <filename>
logFilePut	<hostname> <username> <password> <directory path> <filename>
configFilePut	<hostname> <username> <password> <directory path> <filename>
hostFilePut	<hostname> <username> <password> <directory path> <filename> <ITGFileName>

Note 1: These commands are case-sensitive. The parameters following the command must each be enclosed in quotations marks, and there must be a comma and no spaces between the parameters.

Note 2: For a complete description of these commands, see Table 77: "File Transfer commands" on page 571.

Note 3: Hostname refers to any of the following:

- the IP address of the FTP host
- the Voice Gateway Media Card itself (use loopback address 127.0.0.1)
- another Voice Gateway Media Card

IP configuration commands

Table 65 describes the IP configuration commands.

Table 65
IP configuration commands

IP configuration command	Function
setLeader	Performs all the necessary actions to make a Leader. Sets IP address, gateway, subnet mask, boot method to static, and Leader bit in NVRAM.
clearLeader	Clears the Leader info in NVRAM and sets the boot method to use BOOTP, thus, making the card a Follower.
NVRIPShow	Prints the values of the IP parameters that reside in NVRAM.

Configure TLAN parameters

Auto-negotiate mode can be disabled if the ports on some data network switches and routers are manually configured by the user. For example, configuring a port for 100BaseT Full Duplex can disable auto-negotiation on the signaling link.

The Voice Gateway Media Card and the Internet Telephone default to Half Duplex mode when no auto-negotiation signaling occurs. The result is that the Voice Gateway Media Card and the Internet Telephone operates in Half Duplex mode, while the switch is in Full Duplex mode. Communication continues, but random packet loss can occur which affects the correct operation and voice quality.

> ***Note:*** Set ports for auto-negotiation, auto-sense.

Configure the speed and duplex of the TLAN connection using the following commands:

- **tLanSpeedSet speed**–this command sets the speed of the TLAN interface. By default, the interface auto-negotiates to the highest speed supported by the switch. If the switch is 10/100BaseT, the interface negotiates to 100BaseT. Use this command to debug Ethernet speed-related problems by forcing the interface to 10BaseT operation immediately. The duplex mode setting is saved in NVRAM and read at startup. The parameter speed is set to the following:

  10 - disables auto-negotiation and sets speed to 10 Mbps
  10100 - enables auto-negotiation

- **tLanDuplexSet duplexMode**–this command immediately sets the duplex mode of the TLAN interface while operating when Auto Negotiate is disabled and speed has been fixed to 10 Mbps (or 10BaseT mode). The duplex mode is saved in NVRAM and read at startup. The parameter duplexMode is set to the following:

  0 - enables Full Duplex mode
  1 - enables Half Duplex mode

If disabling the auto-negotiation and forcing the speed and duplex mode using the CLI commands, it is recommended that Half Duplex mode be used to inter-operate with the far end when the far end is set to Auto Negotiate.

If the duplex mode is set to Full Duplex you must guarantee the far end is set to Full Duplex and that Auto Negotiate is off.

Half Duplex mode works with either Half Duplex or Auto Negotiate at the far end. However, Full Duplex at the near end only operates with Full Duplex at the far end.

For the IP Line application, Half Duplex has ample bandwidth for a Voice Gateway Media Card even with 24 busy channels, VAD disabled, and G.711 codec with 10 Mbps voice payload size.

Packet loss monitor

Monitor audio packet loss using the following commands:

- **vgwPLLog 0|1|2**–this command enables the packet loss monitor. Packet loss is measured in the receive direction and the two halves of a call are monitored and logged independently.
  - A value of zero (0) disables packet loss logging.
  - A value of one (1 - default) logs a message if packet loss during the course of the call exceeds the threshold set with the itgPLThreshold command.
  - A value of two (2) indicates that log messages are printed as packet loss is detected during the call. A message is printed each time packet loss is detected indicating how many packets where lost at that moment.
- **itgPLThreshold xxx**–this command sets the packet loss logging and alarm threshold, where xxx is a number between 1 and 1000, and represents the threshold in 0.1% increments. Packet loss which exceeds the threshold, generates an SNMP trap, and writes a message to the log file if logging is enabled. The default value is 10 (1%).

Download the IP Line error log

The ITG error log contains error conditions, as well as normal events. Some error conditions can be severe enough to raise an alarm through SNMP traps.

Use the **LogFilePut** command to download an ITG error log.

Lamp audit and Keep Alive functions

The Lamp Audit function provides a continuous source of heartbeat messages to ensure the Internet Telephone is powered and the IP connection is alive. Since there is a reliable UDP connection from the Meridian 1 and Succession CSE 1000 core through to the Internet Telephones, any failure of the Internet Telephone, the Voice Gateway Media Card, or the IP connection is detected.

You can run Network Signaling Diagnostics as part of the midnight routines. When the Voice Gateway Media Card detects that the Internet Telephone has been disconnected, the Voice Gateway Media Card logs the event and sends an UNREGISTER message to the Meridian 1 and Succession CSE 1000 for that Internet Telephone. When the Meridian 1 and Succession CSE 1000 CPU/Call Server detects a loss of connection with the Voice Gateway Media Card, it logs a message and unregisters all the Internet Telephones and gateway channels associated with that Voice Gateway Media Card.

Table 66 on page 442 summarizes the Meridian 1 and Succession CSE 1000 system administration commands available in LD 32.

Table 66
LD 32 - Administration commands for the Voice Gateway Media Card (Part 1 of 2)

Command	Function
DISC l s c	Disable the specified card, where: l = loop, s = shelf, c = card. ***Note 1:*** You must disable the Voice Gateway Media Card before you transmit card properties from the OTM IP Line 3.0 application. ***Note 2:*** The card reset button is available only in the OTM ITG application when the card is disabled. ***Note 3:*** When you disable the Voice Gateway Media Card in LD 32, it does not disable the active Leader or backup Leader functions.
DISI l s c	Disable the specified card when idle, where: l = loop, s = shelf, c = card ***Note 1:*** This temporarily prevents the IP Telephony node from seizing the port from incoming calls. ***Note 2:*** Use the DISI command to disable the Voice Gateway Media Card instead of the DISC command. The disabled state of the Voice Gateway Media Card is indicated by the NPR0011 message.
DISU l s c u	Disable the specified unit, where: l = loop, s = shelf, c = card, u = unit
ENLC l s c	Enable the specified card, where: l = loop, s = shelf, c = card
ENLU l s c u	Enable the specified unit, where: l = loop, s = shelf, c = card, u = unit
IDC l s c	Print the Card ID information for the specified card, where: l = loop, s = shelf, c = card ***Note 1:*** This command displays the PEC (Product Engineering Code) and serial number for the card. The IP Line PEC is NTZC80AA.

Table 66
LD 32 - Administration commands for the Voice Gateway Media Card (Part 2 of 2)

Command	Function
STAT l s c	Print the Meridian 1 and Succession CSE 1000 software status of the specified card, where: l = loop, s = shelf, c = card
STAT l s c u	Print the Meridian 1 and Succession CSE 1000 software status of the specified unit, where: l = loop, s = shelf, c = card, u = unit

Administration of IP Line Feature Enhancements

Corporate Directory

LD 11 needs to accept CRPA/CRPD class of service input for Internet Telephones.

Table 67
Corporate Directory: LD 11 configuration

Request	Input	Description
REQ:	NEW/CHG	Enter main command.
TYPE:	I2002/I2004/I2005	Enter terminal type.
TN	l s	Enter set TN.
... ...	... ...	... ...
CLs	CPRA/CPRD	Enable/Disable the Corporate Directory feature for this TN.

The Call Server service change does not affect Corporate Directory immediately. If a telephone is in Corporate Directory mode, and there is a service change to set CLS as CPRD, then the current display, and key handling should not be affected. The changed CLS occurs only when the user quits the Corporate Directory application and enters again. For more information about the operation of the Corporate Directory feature, refer to *Installing and Configuring Optivity Telephony Manager* (553-3001-230).

NAT

The Element Management Web server and OTM 2.0 GUIs have two new prompts to configure the timer function:

- Enable NAT support: A checkbox is used to enable or disable the NAT message.
- Keepalive message interval: When NAT is enabled, a configuration box sets the time (in seconds) between messages sent. The default value is 90 seconds. The configured values apply to all Internet Telephones on the node.

Private Zone Configuration

DSP channels and Internet Telephones are set as shared or private based on zone configuration. This is accomplished by adding a new parameter, zoneResourceType, to the zone configuration commands in LD 117.

The new <zoneResourceType> parameter specifies the zone to be either shared or private.

A zone is configured in LD 117 as follows:

NEW ZONE <zoneNumber> [<intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <newResourceType>]

CHG ZONE <zoneNumber> [<intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> <newResourceType>]

By default, a zone is configured as shared (newResourceType=shared).

Virtual Office

The Internet Telephone Virtual Office feature uses the existing Station Control Password (SCPW) feature. The SCPW password can be maintained either by the craftsperson through LD 11 administration or by the user if the Flexible Feature Code (FFC) code access is configured. If the SCPW is not configured for a TN registering by means of the Virtual Office feature, the login is rejected. An appropriate error message is displayed to alert the user that a password must be configured.

Enable the SCPW in the customer data block by setting the length of the SCPW (scpl). The SCPW must be at least four digits.

To login using Virtual Office, the TN associated with the current Internet Telephone registration must be configured with the class of service (CLS) VOLA (Virtual Office Login Allowed). The TN associated with the user id for the login must be configured with the CLS VOUA (Virtual Office User Allowed).

Two new classes of service (CLS) are introduced in LD 11 to restrict Virtual Office usage. The two new classes of services are:

- VOLA/VOLD defines is this TN (physical Internet Telephone) allows/disallows a Virtual Office login option.
- VOUA/VOUD defines if a remote users can log onto this TN (allows/disallows a particular user to login using Virtual Office).

Table 68 on page 446 shows the new CLS for LD 11.

Table 68
LD 11: Virtual Office Login for Internet Telephones

Prompt	Responses	Description	Pkg#
REQ	NEW/CHG		
TYPE	i2002/i2004/i2050	Internet Telephones	
CUST	<number>	Customer number	
BUID	<user id>	Dialable DN, Main Office user id Enter X to delete	390
MOTN	l s c u	Main Office TN for large system Main Office. Accept default for CSE 1000 or Option 11C Main Office	390
...	...	...	
CLS	(VOLA)/VOLD	Virtual Office login operation is allowed/denied on this TN	382, 387
CLS	(VOLA)/VOUD	Allow/Disallow Virtual Office user on this TN using other Internet Telephone	382, 387

802.1Q

The 802.1Q support for Internet Telephones is configured and controlled using the telephone's user interface or DHCP. The DHCP approach eliminates the requirement to manually set the VLAN ID as part of the installation. The configuration is composed of two items: setting the "p" bits and setting the VLAN ID.

The OTM and Element Management's GUI have two fields for setting 802.1Q support:

- Enable 802.1Q support: A checkbox that, when checked, sets the priority bits to the value specified by the next item. If the checkbox is unchecked, the i2002/i2004 Internet Telephone sends out the default priority of 6.
- 802.1Q Bits value (802.1p): A 802.1Q priority bit value field that sets the value the i2002/i2004 Internet Telephones sent out in the priority field. The range is 0 - 7.

IP Line Administration using OTM 2.0

Contents

This section contains information on the following topics:

Reference List

The following are references for this section:

- *Installing and Configuring Optivity Telephony Manager* (553-3001-230)
- *Using Optivity Telephony Manager* (553-3001-330)
- *Upgrades* (553-3023-258)

Overview

This chapter explains how to administer IP Line 3.0 and the Voice Gateway Media Card on the Meridian 1 and Succession Communication Server for Enterprise 1000 Release 1.x systems using OTM.

Optivity Telephony Manager (OTM) provides a graphical user interface to the Voice Gateway Media Card. Use OTM to Telnet to the card, install and upgrade software, configure alarm event reporting, view and update card property and configuration data, add new cards to a node, schedule reports and other related tasks.

WARNING

The only support provided for nodes which reside on a Succession CSE 1000 Rel 2.0 system is the retrieval of OM reports. This is covered in Procedure 60 through Procedure 64.

OTM administration procedures

This section describes the OTM administration procedures using the new OTM **IP Line 3.0** application. All references to OTM in the following procedures assume the latest OTM version.

IP Line Operational Measurement report scheduling and generation

Operational Measurement (OM) reports provide important statistical and traffic information and feedback to the system administrator to better engineer the system. The information stored in the OM file applies only to the calls routed over the IP network by way of IP Line. OM reports give a quantitative view of system performance, such as jitter.

OTM is used to support Operational Measurements on both Meridian 1 and Succession Communication Server for Enterprise (CSE) 1000 systems.

The OM reports are a collection of data from all the Voice Gateway Media Cards in the network. OM data is written to a file every hour. At midnight, the OM file is copied to a backup file, and the new day starts with a new file.

OTM uses the following naming convention for the IP Line 3.0 OM file names:

ipline30_MM_YYYY_file1.csv

Note: The MM (month) portion of the filename is only one character for the months of January to September (1-9). The remaining three months appear as two digit numbers (10, 11, and 12).

An example is ipline30_10_2002_file1.csv. This comma-delimited file opens in a program that interprets the .csv file, such as Microsoft Excel or any other comma-delimited file reader.

The user generates OM reports on demand or on a pre-selected schedule. When a report is generated, the application retrieves the latest OM data from each Voice Gateway Media Card defined in OTM.

Under certain conditions, the OM report is not available:

- the first hour after a Voice Gateway Media Card reboot
- the first hour after installing a new Voice Gateway Media Card

The following error messages are generated when requesting the OM report during the first hour:

- on OTM: "fails to transfer the OM file"
- on the Voice Gateway Media Card console: "tfxl: Error File C:/OM/omreport.xxx not found"

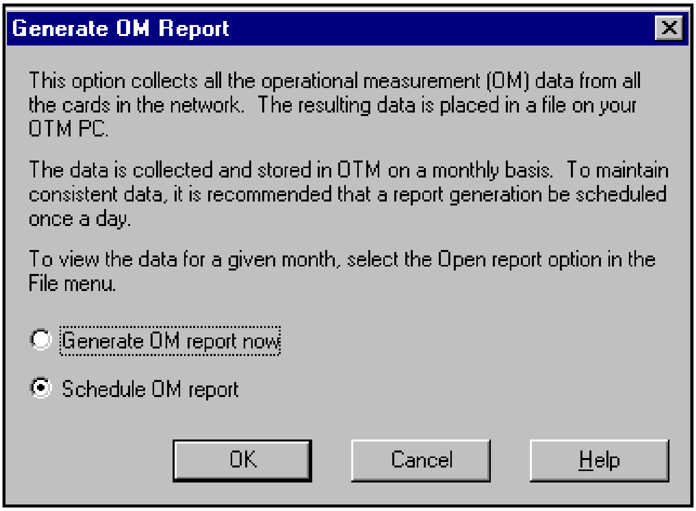
> ***Note:*** Nortel Networks recommends that you schedule report generation once a day.

To schedule a generated OM Report, follow the steps in Procedure 60 on page 453.

Procedure 60
Scheduling Reports

1 Select the node in the **IP Telephony Gateway - IP Line 3.0** window. Click **File | Report | Generate**. The **Generate OM Report** window opens (see Figure 104).

Figure 104
Generate OM Report–Schedule an OM Report

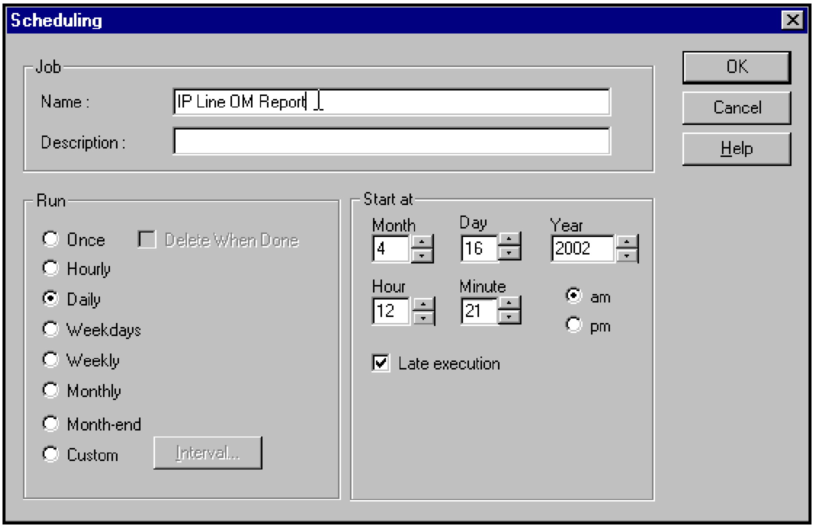


2 In the Generate OM Report window there are two choices, Generate OM report now and Schedule OM report.

3 Select the **Schedule OM report** radio button. Click **OK**.

The **Scheduling** window opens (see Figure 105 on page 454).

Figure 105
Scheduling an OM Report



4 Under **Job**, enter the **Name** and a **Description** for the scheduled OM Report.

5 Under **Run**, select the radio button that indicates the frequency of report generation.

6 Under **Start at**, enter the date and time of the start of the report period using the **Month**, **Day**, **Year**, **Hour**, and **Minute** list boxes and the **am** or **pm** radio buttons.

7 Under **Start at**, click the **Late execution** check box if you want the report to run at a later time in the event the system is busy at the scheduled time.

8 Click **OK**.

End of Procedure

The generated OM report includes information for all cards in all the nodes in the system. The report file accumulates data for the month. The data is stored in the generated file called ipline_MM_YYYY_file#.csv.

OTM has a report feature called "Generate OM Report now". This feature enables an OM Report to be generated immediately.

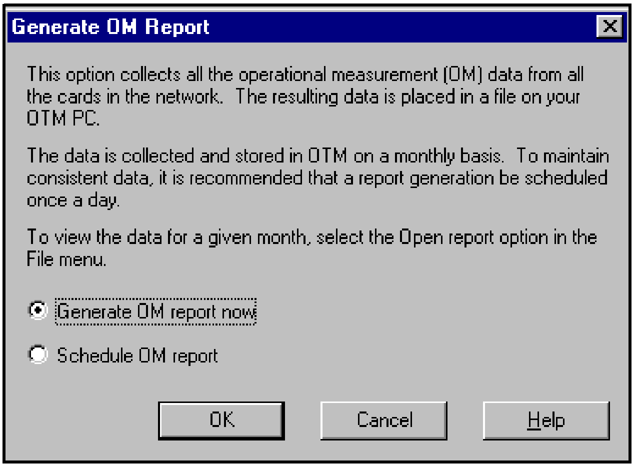
> **WARNING**
> Running the "Generate OM Report now" feature while the Scheduled OM Reports feature is also running causes duplicate data to be displayed at the end of the OM Report. The data for the current day is appended to the end of the OM file by the "Generate OM Report Now" option.
> Be careful to take into account any duplicate data when viewing system performance.

To generate an OM Report immediately, follow the steps in Procedure 61 on page 456.

Procedure 61
Generating reports

1 In the **IP Telephony Gateway - IP Line 3.0** window, click the node. Click **File | Report**. The **Generate OM Report** window opens (see Figure 106).

Figure 106
Generate OM Report–Generate OM report now



2 Click **Generate OM report now** and then click **OK**.

OTM creates and displays a report named **Operational Measurement Report**. This report is saved as a comma-delimited file (csv): ipline30_MM_YYYY_file#.csv. The default file that is generated opens in Microsoft Excel or any other application that can open .csv files.

End of Procedure

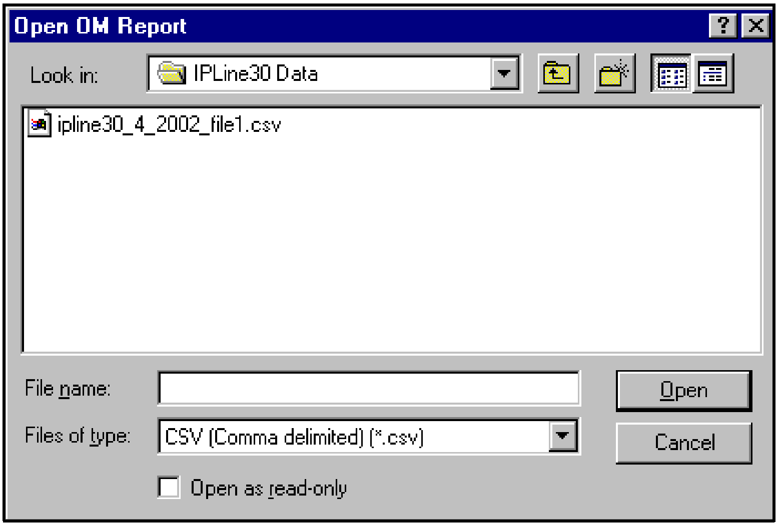
To open and view the OM Report file, follow the steps in Procedure 62 on page 457.

Procedure 62
Opening an Operational Measurement (OM) report

1 In the **IP Telephony Gateway - IP Line 3.0** window, select the node in the top of the window.

2 Click **File | Report | Open**. The **Open OM Report** dialog window opens (see Figure 107 on page 457).

Figure 107
Open OM Report



3 Select a report file and click **Open**. The file opens in a program that interprets .csv (comma-delimited) files such as Microsoft Excel. If Microsoft Excel is not installed on the PC, then OTM notifies the user that the file will be opened in Wordpad.

End of Procedure

You can view OM information for a Voice Gateway Media Card in the node using OTM. This OM file is a view of the TPS and Voice Gateway channel activity on that card. (The OTM OM Report Generation feature is an overview of all the cards in all sites and systems.)

The Voice Gateway Media Card Operational Measurements (OM) file contains the following information:

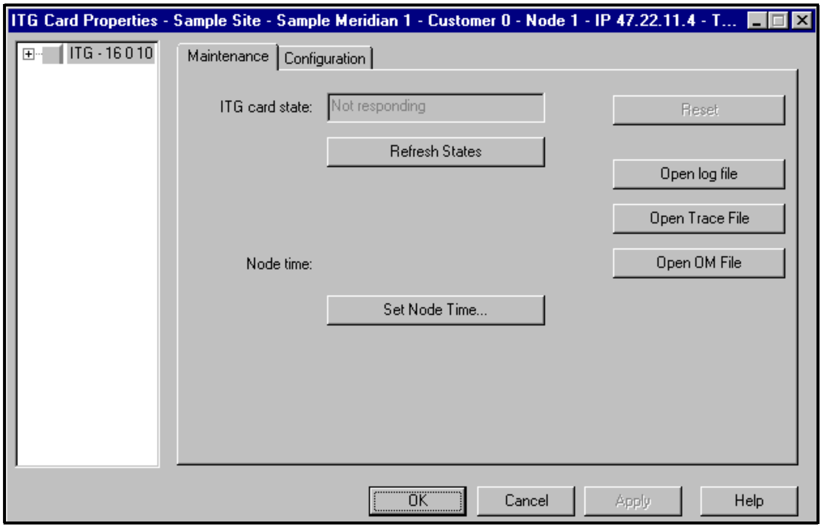
- the number of incoming and outgoing calls
- the number of call attempts
- the number of calls completed
- the total holding time for voice calls

To view a Voice Gateway Media Card's OM file from OTM, follow the steps in Procedure 63 on page 458.

Procedure 63
Retrieving the current OM file from the Voice Gateway Media Card using OTM

1. In the OTM Navigator window, click the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.
2. Select the node in the upper portion of the window. Select the Voice Gateway Media Card from the lower portion of the window.
3. Right-click and then select **Properties** from the pop-up menu. The **ITG Card Properties** window opens to the **Maintenance** tab (see Figure 108 on page 459).

Figure 108
Card Properties–Maintenance tab



4 Click the **Open OM File** button. A file called **om.txt** opens in the WordPad application. The file contains collection period information for each hour of the day that the card was running.

The collection periods start with the hour from midnight to 1:00am. OTM adds to the file each hour, so there is a total 24 collection periods each day. A collection period looks like the following:

collection_time : 2/8/2002 9:00
i2004Reg_Att: 1
i2004Reg_Fail: 0
i2004Unreg_Att: 0
i2004Aud_Setup: 1
i2004Jitter_Avg: 0.1
i2004Jitter_Max: 0
i2004Pkt_Lost: 0.00
i2004Voice_Time: 0 mins 2 secs
ChanAud_Setup: 1
ChanJitter_Avg: 6.0
ChanJitter_Max: 20
ChanPkt_Lost: 0.00
ChanVoice_Time: 0 mins 2 secs
Note: During this collection period, reboot(s) occurred.

Each collection period provides the following:

- the date and time for the collection period hour.
- TPS information for Internet Telephones that are registered to the TPS on the Voice Gateway Media Card during that hour. The TPS information is prefixed by *i2004*.
- Voice Gateway channel information accumulated during the hour. The Voice Gateway data is prefixed by *Chan.*
- Notes indicating whether the machine has been rebooted during the hour.

The om.txt file relates to the omreport.xxx file on the Voice Gateway Media Card, where xxx indicates the numbers of days since December 31.

In general, there is no relationship between the Internet Telephones registered on a card and the Voice Gateway channels on the card (if there are two or more cards) in the node. If there is only one card (with multiple Internet Telephones), there can be a partial correlation between the Internet Telephones and the card information. However, even with only one card there still is not a 100% correlation, since an Internet Telephone can still call another Internet Telephone without involving the Voice Gateway channels.

End of Procedure

Viewing the IP Line log files

OTM uses FTP to transfer the file from the Voice Gateway Media Card to the PC. The file is opened in WordPad. The ITG Error log file (syslog) displays error information, including error date/time, the originating module (IP Telephony node), and specific error data.

To view ITG error conditions that are abnormal events, but not severe enough to raise an alarm, follow the steps in Procedure 64 on page 461:

Procedure 64
Viewing ITG info and error log

1. In the OTM Navigator window, click the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.
2. Right-click in the window. Select **Properties** from the pop-up menu. The **ITG Card Properties** window opens to the **Maintenance** tab (see Figure 108 on page 459).
3. Click the **Open log file** button and review the file contents.

End of Procedure

Back up and restore OTM data

The OTM Backup Wizard is used to backup and restore any or all OTM PC-based data, including IP Line OTM data. All IP Line data is stored in an Access database file on the OTM PC or Server. This file is backed up only when the user selects the “Full OTM Backup” option. This option backs up all OTM data contained in the PC directory where OTM is installed and can only be used to restore all data.

For more information on using the OTM Backup Wizard, see the *Common Services* section in *Using Optivity Telephony Manager* (553-3001-330).

Updating IP Telephony node properties using OTM

To update the node properties of a Voice Gateway Media Card, follow the steps in Procedure 65.

> **CAUTION — Service Interruption**
>
> This procedure is not supported for a node which resides on a Succession CSE 1000 Rel 2.0 system.

Procedure 65
Updating the IP Telephony node properties

1 In the OTM Navigator window, click the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.

2 Double-click on the node in the upper part of the window. The **ITG Node Properties** window appears.

Perform all required updates to the **General** tab and **Configuration** tab parameters. The General and Configuration tabs are used to set the node properties. The other tabs affect the CONFIG.INI file and are also known as the card-affecting properties tabs. If you change any node or card property, you must transmit the configuration data to the node or the card.

3 If you add, delete, or replace Voice Gateway Media Cards from the node or change a Voice Gateway Media Card (refer to the Maintenance section for the procedure to replace a Voice Gateway Media Card), then use one of the following procedures:

- "Adding a Voice Gateway Media Card to the node" on page 463
- "Deleting a Voice Gateway Media Card from the node" on page 469
- "Deleting the Leader Voice Gateway Media Card from the node" on page 471
- "Changing the IP addresses of an IP Telephony node in OTM" on page 472
- "Replacing a Voice Gateway Media Card" on page 599

End of Procedure

Adding a Voice Gateway Media Card to the node

To add a Voice Gateway Media Card to the node, follow the steps in Procedure 66.

CAUTION — Service Interruption

This procedure is not supported for a node which resides on a Succession CSE 1000 Rel 2.0 system.

Procedure 66
Adding a Voice Gateway Media Card to the node

1 Choose a card slot for the new card. Note the TN.

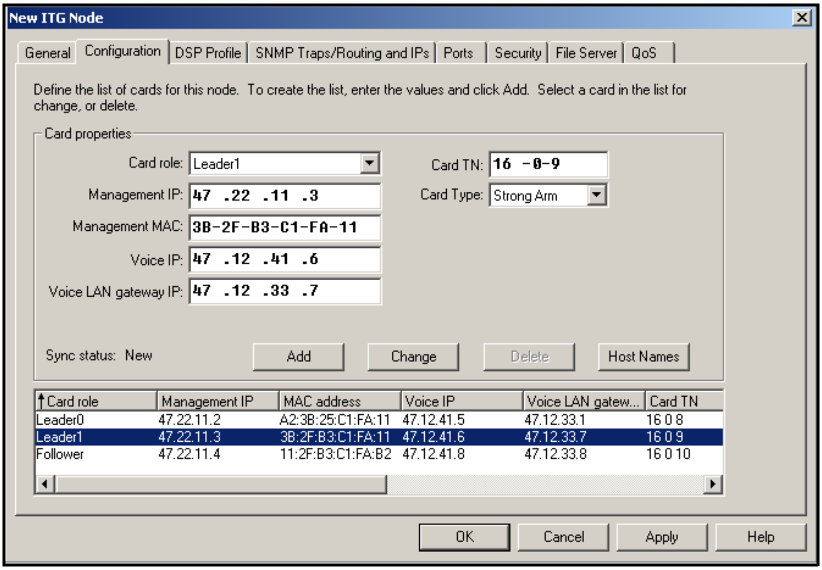
2 Configure IPTN in Meridian 1 and Succession CSE 1000 Rel 1.1 in LD 14 at the Call Server.

3 Install the I/O cables for connection to the ELAN and TLAN on the selected card slot.

4 In the OTM Navigator window, click the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.

5 Double-click the node in the upper portion of the window, the ITG Node Properties window appears. Click on the **Configuration** tab (see Figure 109 on page 464).

Figure 109
Node Properties–Configuration tab



6 Enter the Card Properties data for Leader 1 and the Followers:

a. **Card role:** Assign the Card role Leader 0 to the first card configured. Assign the second card configured as Leader 1. All remaining cards are assigned as Follower.

b. **Management IP:** This is the ELAN IP address for the card. OTM and Meridian 1 and Succession CSE 1000 use this address to communicate with the card.

c. **Management MAC:** This is the motherboard Ethernet address from the "Voice Gateway Media Card installation summary sheet" on page 208.

d. **Voice IP:** This is the TLAN IP address for the card.

e. **Voice LAN gateway IP:** This is the IP address of the router interface on the TLAN.

f. **Card TN:** For Option 51C/61C/81/81C, enter Card TN (l s c) information. For Option 11C and 11C-Mini, enter only the card number between 0-50. The card TN format is determined by the Meridian 1 and Succession CSE 1000 system type that is configured in the OTM Navigator. Enter the correct system type in the OTM Navigator before you add the node.

g. **Card Type:** Select Pentium for the ITG-P Line Card or Strong Arm for the Succession Media Card.

h. Click **Add**. The card role and address information appears in a working list at the bottom of the New ITG Node window.

7 Click **Apply** to add the Card Properties to the Node.

8 If you have more cards, add them by repeating the steps above. Click **OK** when all the cards are added.

Prematurely clicking OK at this point, closes the window and saves any changes. Double-click the new node in the upper part of the main **IP Telephony Gateway - IP Line 3.0** window to re-open Node Properties and complete the configuration procedures.

9 In the OTM Navigator window, click the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.

10 From this list of IP Telephony nodes in the upper part of the window, select the IP Telephony node to which you want to transmit configuration data.

11 Click the **Configuration | Synchronize | Transmit**. The **ITG - Transmit Options** window appears. Keep the default setting of **Transmit to selected nodes** radio button. Check only the **Node Properties to Active Leader** check box (see Figure 110 on page 466).

12 Click the **Start transmit** button. Monitor progress under **Transmit Control** window. Confirm that the node properties are transmitted successfully to Leader 0.

13 When the transmission is complete, click the **Close** button.

14 Choose a card slot for the new card. Note the TN. Configure IPTN in Meridian 1 (see Table 55 on page 253).

15 Install the I/O cables for the connection to the ELAN and TLAN on the selected card slot. Ensure that the I/O cable are connected to the ELAN and TLAN network.

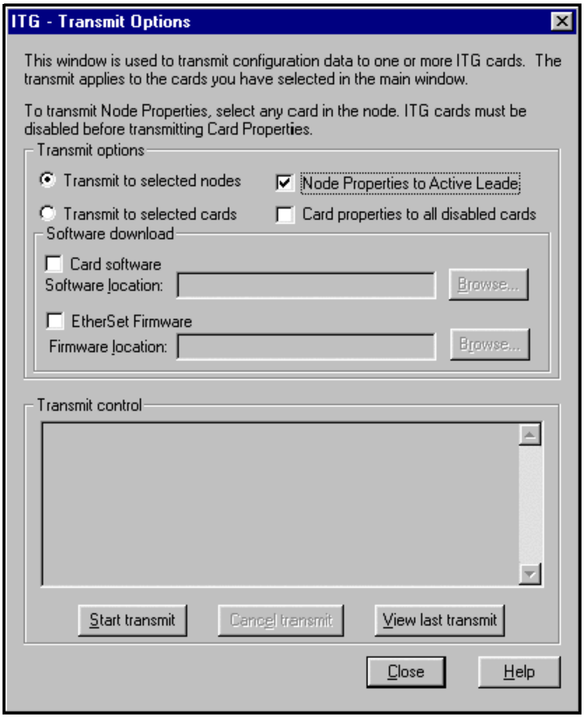
16 In the OTM Navigator window, click the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.

17 From this list of IP Telephony nodes in the upper part of the window, select the IP Telephony node to which you want to transmit configuration data.

18 Click the **Configuration | Synchronize | Transmit**. The **ITG - Transmit Options** window opens.

19 Keep the default setting of **Transmit to selected nodes** radio button. Check only the **Node Properties to Active Leader** check box (see Figure 110 on page 466).

Figure 110
ITG - Transmit Options



20 Click the **Start transmit** button. Monitor the progress in the **Transmit Control** window. Confirm that the node properties are transmitted successfully to Leader 0.

21 When the transmission is complete, click the **Close** button.

22 Insert the new card. The card starts and obtains its IP configuration from the node master. This takes several minutes.

The Maintenance faceplate display shows an alarm of T:21 or S009.

- T:21 is displayed if the card is new and there is no CONFIG.INI file.
- S009 is displayed if the card has been used before and has a CONFIG.INI file that contains an IP address for the Call Server that is no longer correct.

23 In OTM IP Line 3.0 application, refresh the view of the card status in the node. Verify the card is responding to OTM by selecting the IP Telephony node from the list in the upper part of the main window. All Voice Gateway Media Cards in the node are displayed in the lower part of the window. While the node is selected, from the node list, press function key **F5** or **View | Refresh | Selection** to refresh the card status of all cards in the selected node.

The card status should display as “Enabled” or "Disabled". If the status is “Not responding”, verify the network connection and the proper configuration of the network equipment.

24 In the OTM Navigator window, click the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.

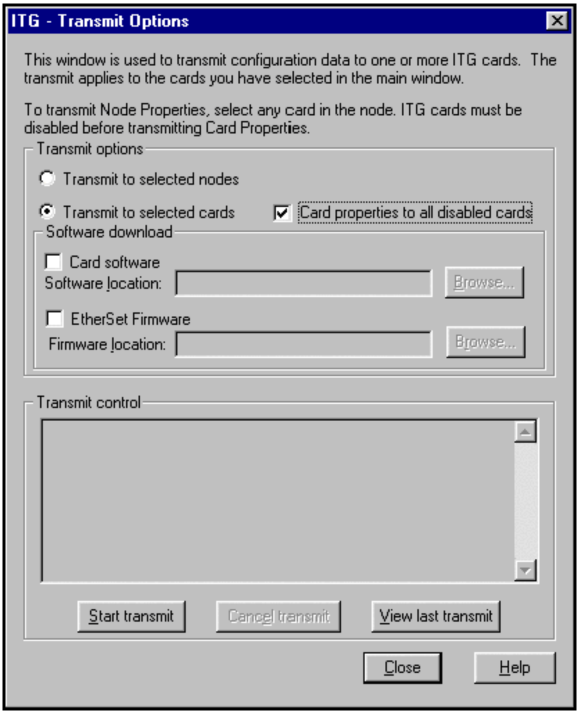
25 Select the IP Telephony node in the upper part of the window.

26 Select the new card(s) in the lower part of the window. Use the **Ctrl** key to select multiple cards.

27 Click the **Configuration** menu option and then select **Synchronize | Transmit**. The **ITG - Transmit Options** window appears.

28 Click the **Transmit to selected cards** radio button and the **Card Properties to all disabled cards** check box (see Figure 111 on page 468).

Figure 111
ITG - Transmit Options



29 Click the **Start transmit** button. Monitor the progress in the **Transmit Control** window.

30 When the transmission is complete, click the **Close** button.

31 Verify that all the new Voice Gateway Media Cards in the node have a signaling link to the Call Server.

32 Telnet to each Voice Gateway Media Card and log in. At the IPL> command line, enter the **pbxLinkShow** command. You can also look at the display on the card and ensure it is displaying F000.

33 At this point you must verify the card loadware and firmware version. Upgrade the loadware and the firmware, if necessary, using Procedure 27 on page 309, Procedure 28 on page 314, and Procedure 30 on page 318. However, apply these procedures only to this card.

End of Procedure

Deleting a Voice Gateway Media Card from the node

To delete a Voice Gateway Media Card from the node, follow the steps in Procedure 67.

To delete the Leader 0 Voice Gateway Media Card from the node, follow the steps in Procedure 68 on page 471.

CAUTION — Service Interruption

These procedures are not supported for a node which resides on a Succession CSE 1000 Rel 2.0 system.

Procedure 67
Deleting a Voice Gateway Media Card from the node

1 In the OTM Navigator window, click the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.

2 Select the node in the upper portion of the window.

3 In the **IP Telephony Gateway - IP Line 3.0** window, select **Node | Properties** from the popup menu. The ITG Node Properties window is displayed.

4 Click the **Configuration** tab.

5 Select the Voice Gateway Media Card to be deleted from the working list at the bottom of the window.

6 Click the **Delete** button.

7 Click **OK**.

8 Next transmit the node properties. In the **IP Telephony Gateway - IP Line 3.0** window, click the **Configuration | Synchronize | Transmit**. The **ITG - Transmit Options** window opens.

9 Select the **Transmit to selected nodes** radio button. Check the **Node Properties to Active Leader** check box.

10 Click the **Start transmit** button. Monitor progress in the **Transmit Control** window. Confirm that the node properties are transmitted successfully to Leader 0.

11 When the transmission is complete, click the **Close** button.

12 Remove the Voice Gateway Media Card.

> **CAUTION WITH ESDS DEVICES**
> Follow the anti-static procedures and place the Voice Gateway Media Card in an appropriate anti-static package.

13 Remove the Voice Gateway Media Card configuration data from the Call Server.

- **a.** Identify the TN of the Voice Gateway Media Card.
- **b.** In LD 20, enter the **LTN** (List Terminal Number) command where TYPE = tie, to list the TNs on the Voice Gateway Media Card TN. This returns a list of units equipped on the card. Verify the number of units that are equipped on the card. Take note of the first unit equipped on the card.
- **c.** In LD 14, use the **Out n** command, where **n** equals the number of units that are equipped on the card.

14 At the TN prompt, enter the TN for the first unit that was equipped on the card as determined in Step 15. As the units are deleted, verify that you have “outed” the intended units.

End of Procedure

Deleting the Leader Voice Gateway Media Card from the node

A node's Leader 0 card cannot be deleted from OTM. The user must Telnet to the Leader 0 Voice Gateway Media Card and enter a command to remove the Leader 0 card. Follow the steps in Procedure 68 to delete the Leader 0 card.

> **CAUTION — Service Interruption**
>
> This procedure is not supported for a node which resides on a Succession CSE 1000 Rel 2.0 system.

Procedure 68
Deleting the Leader 0 Voice Gateway Media Card from the node

1 In the OTM Navigator window, click the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.

1 Select the node in the upper portion of the window.

2 In the lower portion of the window, right-click on the Leader 0 card that will be deleted. Select **Telnet** from the pop-up window.

3 Log in to the card.

4 Enter the **clearLeader** command from the IPL> CLI. This command removes the IP address information from NVRAM and also clears the Leader flag.

End of Procedure

Changing the IP addresses of an IP Telephony node in OTM

Prior to changing any IP address, ensure that you understand the "IP Network Engineering Guidelines" on page 133, and consult with the IP network administrator. IP address configuration changes are completed on four tabs in the ITG Node Properties window. The four tabs are:

- General tab – Configure network connections in this tab.
  See Figure 112 on page 473.
- Configuration tab – Card properties are set in this tab.
  See Figure 113 on page 475.
- SNMP Traps/Routing and IPs tab – SMNP traps and card routing table entries are configured in this tab.
  See Figure 115 on page 478.
- Ports tab – ELAN settings are set in this tab.
  See Figure 116 on page 479.

To change the IP address of an IP Telephony node, follow the steps in Procedure 69 on page 472.

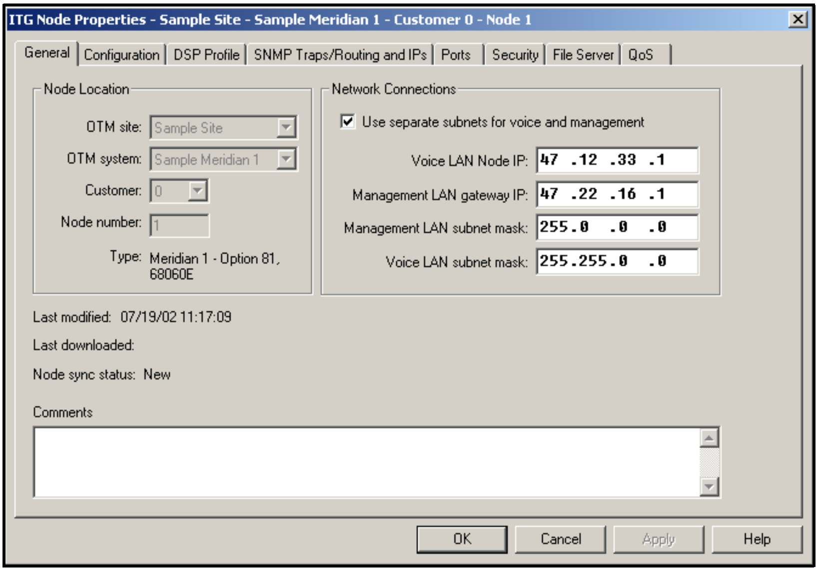
CAUTION — Service Interruption

This procedure is not supported for a node which resides on a Succession CSE 1000 Rel 2.0 system.

Procedure 69
Changing the IP addresses of an IP Telephony node in OTM

1. In the OTM Navigator window, click the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.
2. Select the node in the upper portion of the window. Select the card in the lower portion of the window.
3. Click **Configuration | Node | Properties** to update the Voice Gateway Media Card IP addresses as required. The **ITG Node Properties** window opens.

Figure 112
Node Properties–General tab



4 Select the **General** tab (see Figure 112 on page 473).

Under **Network Connections**:

a. Never uncheck "Use separate subnets for voice and management".

b. **Voice LAN Node IP:** This is also known as the TLAN IP address.

- If the node IP is changed, this affects the configuration of the Connect Server IP address in the DHCP Server for the Internet Telephones.
- If the Internet Telephones are using partial DHCP mode, manually reconfigure the IP address in each Internet Telephone.

c. **Management LAN gateway IP:** This IP address is used to route to the ELAN. If OTM is not connected to the local ELAN, then it communicates with this node through the Management LAN gateway. If you make changes to the gateway IP address and these changes are not coordinated properly, OTM loses communication with the node:

- When a Management LAN gateway is added to the ELAN, it must restrict access so that only authorized traffic is permitted on the ELAN.
- The router must disable the BootP relay agent for ELAN interface.
- The router must block all broadcast and multicast traffic from the ELAN and enable only proper access, that is, only authorized traffic and users coming through the Management LAN gateway. OTM is one of these users.

d. **Management LAN subnet mask:** When changing these subnet masks, consider the possibility of conflict between the ELAN and TLAN IP addresses. Consult with the IP administrator before making any changes to subnets. See "IP Network Engineering Guidelines" on page 133.

When changing the Management LAN (ELAN) subnet, this must be coordinated with the IP address on the Call Server (Active ELNK) subnet. You must also coordinate changes with the following:

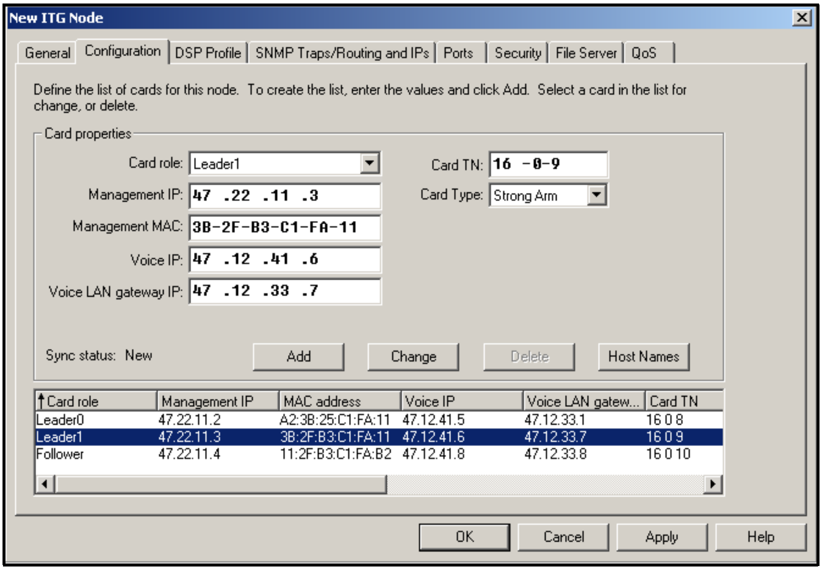
- Management LAN gateway, and other IP devices on the ELAN (for example, OTM if it is local)
- any other devices on the ELAN and the customer's enterprise network (CLAN) that should need to communicate with IP Line
- devices that are looking to receive SNMP traps

e. **Voice LAN subnet mask:** Coordinate with Voice LAN gateway (router). When changing the Voice LAN (TLAN) subnet mask, the change must be coordinated with changing the subnet mask of the Voice LAN (TLAN) gateway (router) interface.

5 Click **Apply**.

6 Select the **Configuration** tab (see Figure 113 on page 475).

Figure 113
Node Properties–Configuration tab

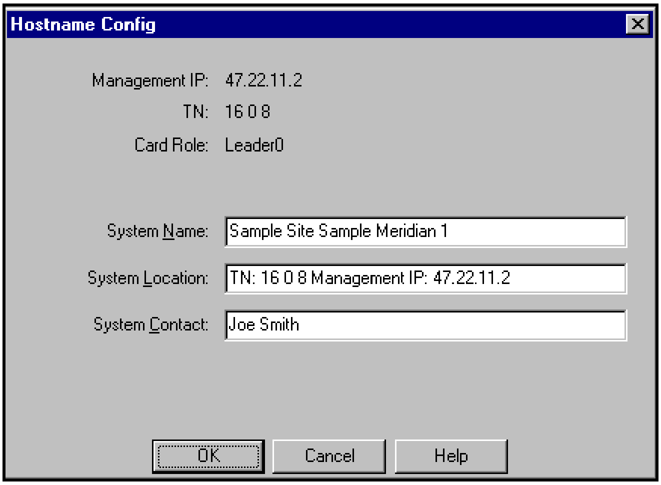


7 Select the card to be changed from the list at the bottom of the tab.

8 Click the **Host Names** button. The Hostname Config window opens (see Figure 114 on page 476).

The Hostname Config is part of the management information base. It enable the card to be identified by System Name, System Location, and System Contact to an SNMP management server. If you need to change any of these items, you must change them on each individual card. Click **OK** when done to return to the Configuration tab.

Figure 114
Hostname Config



9 Under **Card Properties**:

a. **Card Role:** The first card in the node must exist. This card is Leader 0.

Every IP Telephony node must have only one Leader 0. All other cards function as Followers. OTM, however, requires that the first Follower be configured as Leader 1 even though it has no Leader functions. The remaining cards are configured as Followers.

b. **Management IP:** If you are changing the Management IP address of Leader 0, you must Telnet to the card and use the setLeader command to make the same change (new Management IP address) in the NVRAM of the Leader 0 card.

Leader 0 must be reset for OTM to resume communication with the node.

Note: Prior to resetting Leader 0, unplug all the other cards to prevent any other card from becoming the Master. When Leader 0 restarts, plug the cards back in. These other cards receive their new configuration for Leader 0.

c. **Management MAC:** All other IP configuration depends on the accurate configuration of the Management MAC address. The MAC address is located on the faceplate of the Voice Gateway Media Card and is labelled as MOTHERBOARD Ethernet address. The Management MAC address corresponds to the ELAN address.

d. **Voice IP:** This is the card voice IP address. This address is also known as the card TLAN IP address. In an IP Telephony node, all cards must be assigned an address on the same TLAN subnet. The card voice IP address must be distinct from the node IP address.

e. **Voice LAN gateway IP:** All cards in the IP Telephony node must be on the TLAN; therefore they all share the same Voice LAN / TLAN gateway IP address.

f. **Card TN:** It is mandatory that the Card TN format match both the machine type and the card slot where the card resides. Otherwise, the voice gateway channels do not function.

   If you are trying to change the card TN format, first record the node configuration data. Delete the node. Change the card TN format to the correct machine, and rebuild the node.

   For Option 51C/61C/81/81C systems, enter Card TN (l s c) information. For Option 11C, 11C-Mini, and Succession CSE 1000 systems, enter only the card slot number between 1-50. The card TN format is determined by the Meridian 1 and Succession CSE 1000 system type which is configured in the OTM navigator. You must enter the correct system type in the OTM Navigator before you add the node.

g. **Card Type:** Select Pentium for the ITG-P Line Card or Strong Arm for the Succession Media Card.

10 For each card:

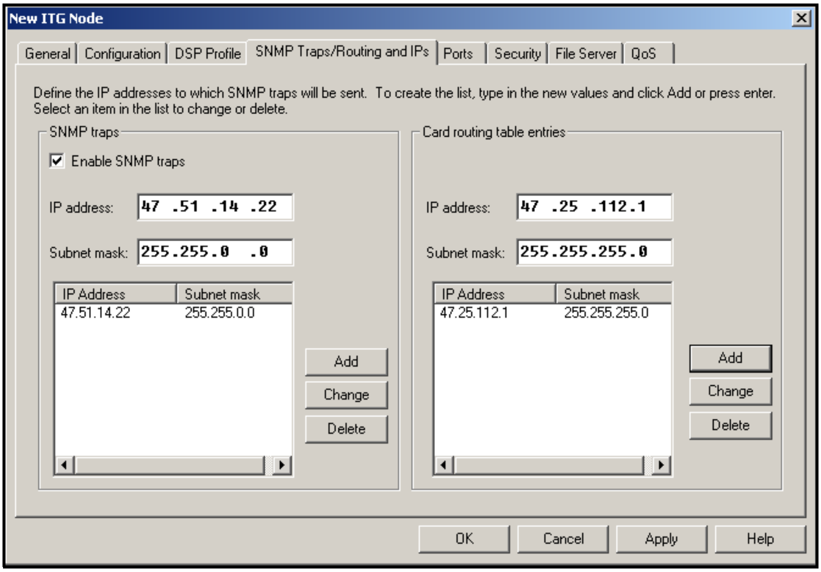
   i. Click the **Change** button. The changes are reflected in the working list at the bottom of the tab.

   ii. Then click **Apply** to save the changes to the card in the database.

Select the next card to be changed from the working list at the bottom of the tab, make the appropriate changes, and then repeat the above steps.

11 Select the **SNMP Traps/Routing and IPs** tab (see Figure 115 on page 478).

Figure 115
Node Properties–SNMP Traps/Routing and IPs



Changes can be made to the SNMP Traps and Card routing table entries without affecting other IP addresses. Change the SNMP traps and Card routing table entries as required, based on the destination host you are trying to reach.

IP addresses that are added in this tab create special card routing tables that direct packets out the ELAN and ELAN gateway. Exercise caution when adding entries since the entry could result in one-way voice transmission if a change results in voice packets being streamed out the ELAN instead of the TLAN interface.

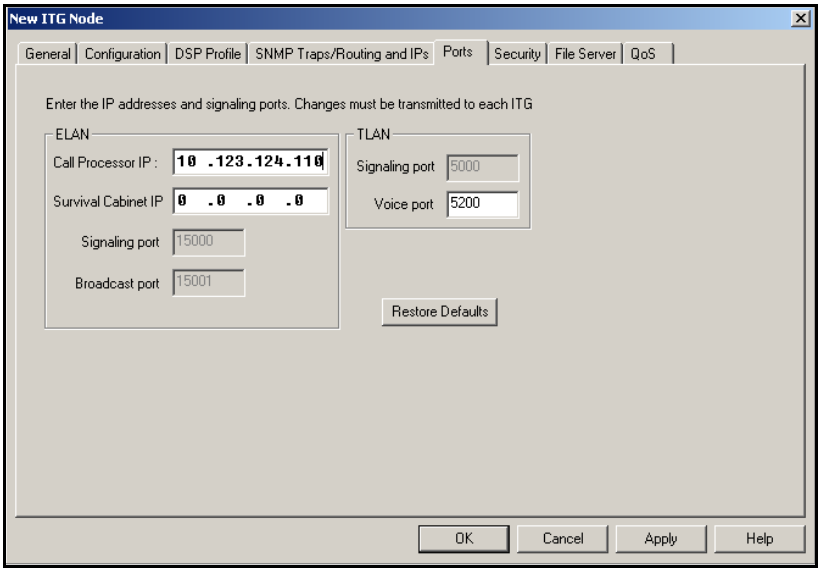
Under **SNMP Traps**, configure up to eight SNMP trap servers can be defined.

Under **Card routing table entries**, use caution when assigning card routing table entries. Do not include the IP address of an Internet Telephone. Otherwise, voice traffic to these Internet Telephones is incorrectly routed through the ELAN and ELAN gateway. To avoid including the wrong IP address it is recommended that you define Host IDs for the card routing table entries.

12 Click **Apply**, if any changes are made on the SNMP Traps/Routing and IPs tab.

13 Select the **Ports** tab (see Figure 116 on page 479).

Figure 116
Node Properties–Ports tab



Under **ELAN**:

a. **Call Processor ID:** A change to this IP address must be coordinated with the Call Server (Active ELNK) subnet.

b. **Survival Cabinet IP:** If applicable, enter the Survivable Cabinet ELAN IP address (Active ELNK). The survivable Cabinet IP is enabled only for Option 11C and Succession CSE 1000 systems.

Note: For Option 11C, Option 11C-Mini, or Succession CSE 1000, this field is disabled unless you have defined at least one cabinet as a survival cabinet of the main system in OTM Navigator. There is only one survival cabinet IP address for each node. The survivable cabinet is equipped with sufficient Trunk cards and Voice Gateway Media Cards. In case of Call Server equipment failure, it provides a large degree of survivability for Internet Telephone users.

c. **Signaling port:** This field is read-only.

d. **Broadcast port:** This field is read-only.

Under **TLAN**:

a. **Signaling port:** This field is read-only.

b. **Voice port:** This field displays the range for RTP packets sent to the Internet Telephones. In general, use the default value of 5200. If, however, there are numerous telephones working over low bandwidth WAN links using CISCO RTP header compression, then change the voice port to a number in the range of 16384 to 32767. Coordinate this value change with your IP network administrator.

14 Click **Apply**.

15 When all updates to the IP addresses have been made, click **OK** in the ITG Node Properties window.

16 Unplug all the Voice Gateway Media Cards, except Leader 0. Leader 0 receives its configuration from the BOOTP.TAB file. Plug in all the cards. Leader 0 forces its configuration to all the other cards.

17 You must now transmit the node or card properties to the Leader 0 card.

Select the Leader 0 Voice Gateway Media Card in the IP Telephony Gateway - IP Line 3.0 window.

If changes are made to the __________ tab...	... then you must transmit ___________ properties.
General ***Note:*** If changes are made to the System Name, System Location, or System Contact in the Hostname Config window (Host Names button) you must transmit the card properties.	node
Configuration	node
SNMP Traps/Routing and IPs	card
Ports	card

18 Click the **Configuration | Synchronize | Transmit**.

To transmit to the node, select the **Transmit to selected nodes** radio button. Check the **Node Properties to Active Leader** check box.

Click the **Start transmit** button.

The results of the transmit appear in the box under **Transmit control**. Verify that the properties are transmitted successfully. If the transmit is unsuccessful, click the **Start transmit** button again.

19 Login to LD 32 and disable the cards using the DISI command.

Click the **Configuration | Synchronize | Transmit**.

Select the **Transmit to select cards** radio button. Check the **Card Properties to all disabled card** check box.

Click the **Start transmit** button.

The results of the transmit appear in the box under **Transmit control**. Verify that the properties transmitted successfully. If the transmit is unsuccessful, click the **Start transmit** button again.

20 Click **Close** when the properties are successfully transmitted.

If the IP addresses of a single card have changed, the card must be restarted for the changes to take effect (see "Restarting a Voice Gateway Media Card" on page 482). However, if IP addresses that affect the entire node have been changed, then all cards in the node have to be restarted (see "Restarting all Voice Gateway Media Cards" on page 483).

Restarting a Voice Gateway Media Card

If the IP address of a Voice Gateway Media Card has changed, restart that card only.

1. To prevent interruption to the speech path, login to LD 32. Type the **DISI** command. This command disables the voice gateway channels when they become idle. DISI removes the call traffic but does not remove the Internet Telephones that are registered on that Voice Gateway Media Card. The Graceful TPS Disable command does this.

2. Type **disiTPS** at the card's IPL> prompt to disable the TPS service on the Voice Gateway Media Card. This Graceful TPS Disable command prevents new Internet Telephones from registering on the card. All Internet Telephones registered on the card are redirected to another Voice Gateway Media Card when the telephone becomes idle.

   After the command is entered, an idle Internet Telephone is supposed to be updated with the Watchdog reset message. However, the TPS sends a soft reset message to the Internet Telephone, redirecting it to the Connect Server. The disabled TPS does not accept new registrations, so the Internet Telephones must register with another TPS in the node. Eventually, as all of the TPS's Internet Telephones become idle, they are registered with other TPSs. The Voice Gateway Media Card can then be restarted with no impact to any users.

Restarting all Voice Gateway Media Cards

All cards have to be restarted if there has been a change to the following:

- node IP address
- subnet of either the TLAN or ELAN (by changing the subnet mask or the subnet fields of the IP address)

These changes affect the whole node and, as a result, all cards must be restarted.

If the Management IP address of Leader 0 has changed, all cards have to be restarted. Even though this is a change to a single card, this change affects all cards, as OTM uses this address to transmit properties to the node:

1. Telnet to the card from OTM.
2. Use the **setLeader** command to set the new IP address. Leader 0 uses this new IP address when it reboots.
3. Reboot the Leader 0 using the **cardReset** command.
4. The Leader 0 card reads the new IP address from NVRAM.
5. Restart all the other cards.

End of Procedure

Update Voice Gateway Media Card card properties

Some basic Voice Gateway Media Card configuration must be performed from the ITG Node Properties window. To update the card properties in the DSP Profile, follow the steps in Procedure 70.

CAUTION — Service Interruption

This procedure is not supported for a node which resides on a Succession CSE 1000 Rel 2.0 system.

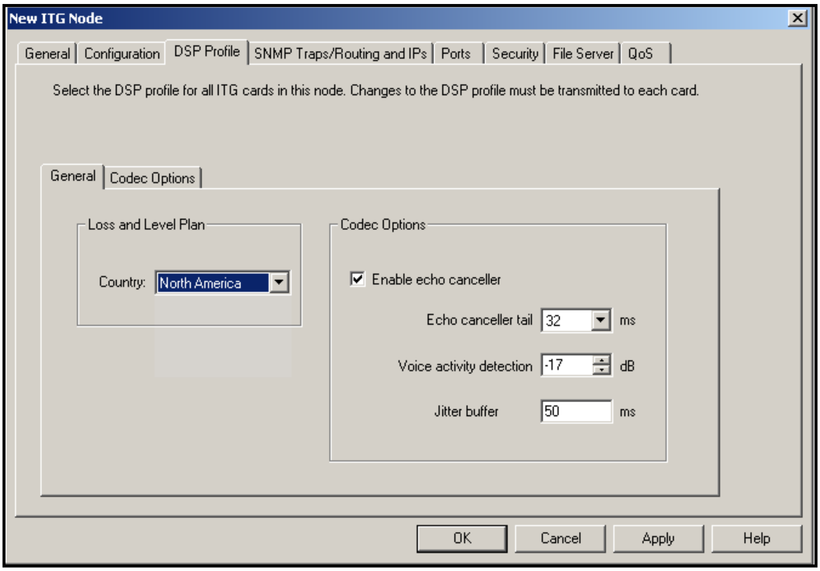
Procedure 70
Updating card properties–DSP Profile tab

1 In the OTM Navigator window, click the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.

2 Click **Configuration | Node | Properties**.

3 Click the **DSP Profile** tab. The **General** sub-tab appears (see Figure 117 on page 484).

Figure 117
Node Properties–DSP Profile tab–General sub-tab



4 Under **Loss and Level Plan**, select your **Country** from the pull-down box.

5 Under **Codec Options**, use the default settings unless indicated as follows or directed to change them by Nortel Networks Field Support.

a. **Enable echo canceller:** Leave checked.

b. **Echo canceller tail:** Select the maximum value.

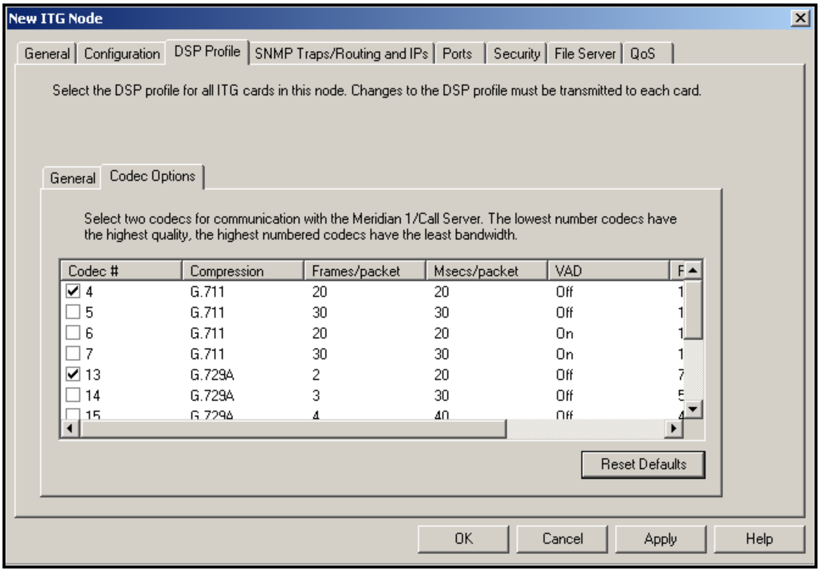
c. **Voice activity detection:** The default value is –17. The range is –20 to +10 dB

d. **Jitter buffer:** The default is 50ms. The range is 0 ms to 200 ms and this is determined by the codec (see “Adjusting jitter buffer size” on page 189).

6 Click **Apply**.

7 Click the **Codec Options** sub-tab (see Figure 118 on page 485).

Figure 118
Node Properties–DSP Profile tab–Codec Options sub-tab



Note 1: The Codec Options sub-tab contains a list of up to 32 codec settings for G.711, G.729A, and G.729AB for the Voice Gateway Media Card. Select exactly two codecs from the **Codec #** list.

The default Codec # settings are 4 and 17.

The Codec # indicates a particular codec (G.711 or G.729A) with different options for Frame Size and VAD (On or Off).

The lower of the two Codec #s that you check corresponds to BQ (Best Quality) and BB (Best Bandwidth) in LD 17.

For example, if you select Codec # 13 and Codec # 14:

- Codec # 13 corresponds with Best Quality
- Codec # 14 corresponds with Best Bandwidth

Note 2: If there are multiple nodes on a system and the same codec is selected on more than one node, ensure that each node has the same voice payload size configured for the codec.

8 Click **Apply** and then click **OK**.

End of Procedure

As a result of the new Run-time Configuration Change feature, the card does not have to be restarted if there are changes to the settings on the DSP Profile tab. For changes to the Codec Options, or Loss and Level Plan settings on the DSP Profile tab, disable the card, download the card properties, and then re-enable the card.

If the settings have changed on the DSP Profile tab, follow the steps in Procedure 71 to disable and then enable the Voice Gateway Media Card.

CAUTION — Service Interruption

This procedure is not supported for a node which resides on a Succession CSE 1000 Rel 2.0 system.

Procedure 71
Disabling and re-enabling the Voice Gateway Media Card

1. Changes to the DSP Profile tab settings are applied immediately when the card properties are transmitted.

   Login to LD 32 on the Call Server and use the **DISI** command to disable the Voice Gateway Media Card.

2. In the OTM Navigator window, click the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.

3. Select the IP Telephony node from the list in the upper part of the main window. All Voice Gateway Media Cards in the node are displayed in the lower part of the window. Select the node from the node list and press function key **F5** or **View | Refresh | Selected** to refresh the card status of all cards in the selected node.

4. In the **IP Telephony Gateway - IP Line 3.0** window, click the **Configuration** menu option and then select **Synchronize | Transmit**. The **ITG - Transmit Options** window appears.

5. Select the **Transmit to selected cards** radio button. Check the **Card Properties to all disabled cards** check box.

6. Click the **Start transmit** button. Verify that the transmit is successful under **Transmit Control** and then click **Close**.

7. Login to the Call Server and go to LD 32. Type the **ENCL** command to enable the Voice Gateway Media Card.

End of Procedure

Using the Retrieve command

The Retrieve command sends information from the Voice Gateway Media Cards to the OTM IP Telephony node. The Retrieve command is used for:

- downloading a node or card configuration by a remote OTM user

  Note: This can also be performed by doing the “Add ITG Node” command and selecting the “Retrieve the active configuration from an existing node” option.

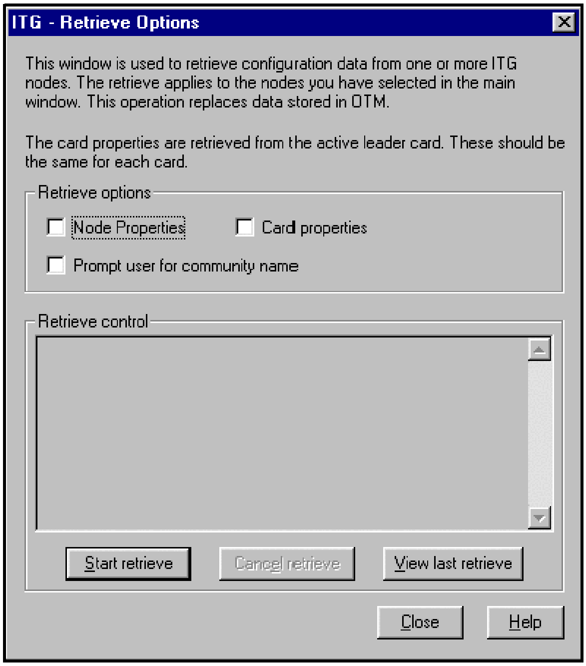
- copying node information from one node to another
- restoring accidentally changed OTM information, and downloading information to a fictitious “dummy” node that has been created for this purpose, in order to view the configuration of the Voice Gateway Media Card and the IP Telephony node.

> **CAUTION — Service Interruption**
>
> This procedure is not supported for a node which resides on a Succession CSE 1000 Rel 2.0 system.

Procedure 72
Using the Retrieve command

1. In the OTM Navigator window, click the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.
2. Select the card(s) from which to retrieve information.
3. Click **Configuration | Synchronize | Retrieve**. The **ITG - Retrieve Options** window opens (see Figure 119 on page 489).

Figure 119
ITG - Retrieve Options



4 Under **Retrieve Option**, configure whether to retrieve **Node properties** or **Card properties** by clicking one or more of the check boxes.

5 Click **Start Retrieve**. The results of the Retrieve command are displayed under **Retrieve control**.

Note 1: If the Retrieve command is successful, the current configuration of the node or card properties in OTM is overwritten by the configuration data that was retrieved from the node. The new configuration data can be viewed in the ITG Node Properties window.

Note 2: If you want to view the configuration of a node without overwriting the current node configuration in OTM, retrieve the information to a dummy node.

End of Procedure

Adding an IP Telephony node in OTM by retrieving an existing node

Use this optional procedure in the following cases:

- Add existing nodes to a particular OTM PC to manage the ITG network from a single point of view.
- Restore the ITG configuration database to an OTM PC whose hard drive has crashed, as an alternative to restoring the OTM IP Telephony nodes from the OTM Disaster Recovery Backup.

When you install and configure the IP Telephony node manually, you can then add that node to another OTM PC by retrieving the configuration data from the existing IP Telephony node.

Make sure that you configure the site name, system name, and customer number in the OTM Navigator before you add a new IP Telephony node. Only one IP Telephony node can be added in the OTM ITG application for each Meridian 1 and Succession CSE 1000 customer.

If multiple OTM PCs are used to manage the same ITG network, care must be taken to synchronize the different copies of the ITG database. The OTM ITG **Configuration | Synchronize | Retrieve** function can be used to synchronize the OTM ITG database with the database on the IP Telephony node.

CAUTION — Service Interruption

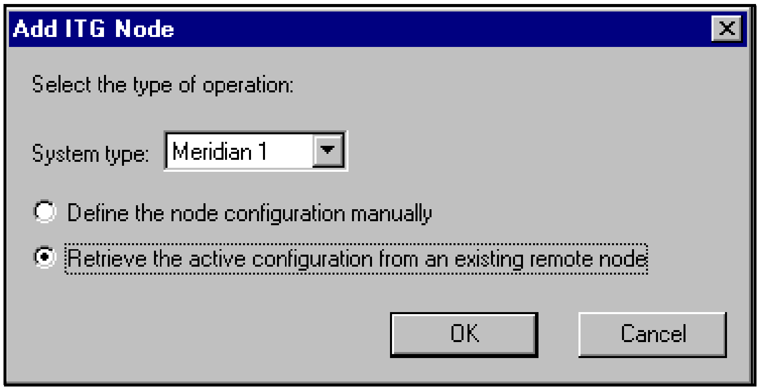
This procedure is not supported for a node which resides on a Succession CSE 1000 Rel 2.0 system.

Procedure 73
Configuring the node and Leader 0

1 In the OTM Navigator window, click the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.

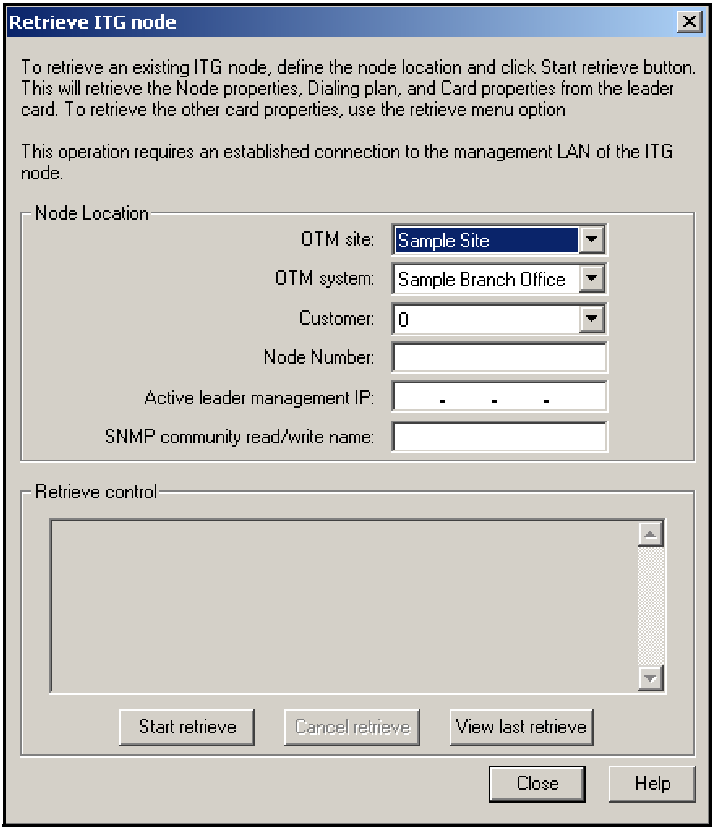
2 Click the **Configuration | Node | Add**. The **Add ITG Node** dialog box (see Figure 120 on page 491) opens.

Figure 120
Add ITG Node–Retrieve configuration from existing node



3 Click the **Retrieve the active configuration from an existing remote node** radio button, and then click **OK**. The **Retrieve ITG node** window opens (see Figure 121 on page 492).

Figure 121
Retrieve ITG node



4 The OTM site name, OTM system name, and customer number must exist in the OTM Navigator before you can add a new IP Telephony node.

Note: Ensure the Meridian 1 system type, for example, Option 81C, Option 11C, and Succession CSE 1000 is defined correctly.

Under **Node Location** in the **Retrieve ITG node** window:

a. **OTM site:** Select the OTM Site.

b. **OTM system:** Select the Meridian 1 System.

c. **Customer:** Select the Meridian 1 Customer number.

d. **Node Number:** Ensure the node number is unique under the Meridian 1 customer number. Also, ensure that all IP Telephony nodes connected to the same TLAN subnet have a unique node number regardless of the OTM site, Meridian 1 system, and customer number.

e. **Active leader management IP:** Enter the active Leader management IP address field for the existing node.

f. **SNMP community read/write name:** Enter the SNMP read/write community name.

5 Click **Start retrieve**.

The results of the retrieval are shown under **Retrieve control**. The node properties are retrieved from the active Leader. The card properties are retrieved from Leader 0.

6 Click **Close** when the download is complete.

7 In the **IP Telephony Gateway - IP LIne 3.0** window, select the newly added node in the top part of the window.

8 Refresh the card status (**View | Refresh**) and verify that the cards in the newly added node are responding.

9 A new node has been created by retrieving data from another node Double-click on the new node in the **IP Telephony Gateway - IP Line 3.0** window. The **ITG Node Properties** window opens for the newly added node.

10 Inspect each tab in the node properties and verify the data is correct and consistent with the node from which you retrieved the data. Click the **Configuration** tab, ensure the Host names information, IP addresses, and TN are consistent.

End of Procedure

IP Line Command Line Interface access using Telnet or local RS-232 maintenance port

There are two ways to access the IPL> Command Line Interface (CLI):

1 Use the NTAG81CA cable to connect the DIN8 pin connector on the faceplate, or the NTAG81BA cable to connect the DB9 I/O breakout cable to the COM port of a local PC. Use a null modem adapter to connect a modem for remote dial-up access.

2 Telnet to the card from the OTM **IP Telephony Gateway - IP Line 3.0** window. This automatically Telnets to the IP address of the management interface (ELAN) of the card. You can also use the Telnet application on your computer and manually enter the management IP address (ELAN), voice IP address (TLAN), or the node IP address if you are trying to connect to the active Leader.

CAUTION
Do not connect two maintenance terminals to both the faceplate and I/O panel serial maintenance port connections at the same time.

Telnet to a Voice Gateway Media Card

To access the command line on a Voice Gateway Media Card from the OTM PC, perform Procedure 74 on page 494.

Procedure 74
Accessing a Voice Gateway Media Card using Telnet

1 In the OTM Navigator window, click the **Services** folder. Double-click the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.

2 Right-click on the Voice Gateway Media Card that you want to access. Select **Telnet to ITG card** from the popup menu. OTM PC opens a Telnet window and automatically connects to the Voice Gateway Media Card by using the management IP address (ELAN).

3 Enter a username and password to access the IPL> CLI. The default user name and password are both **itgadmin**. However, the user name and password should have been changed during installation.

4 The IPL> prompt appears if the login is successful. Type **?** at the prompt to display a list of available IPL> CLI commands. See “IP Line CLI commands” on page 567 for a detailed list of commands.

End of Procedure

IP Line Administration using Element Management

Contents

This section contains information on the following topics:

Reference list

The following are references for this section:

- *Element Management* (553-3023-222)

Overview

This chapter explains how to administer IP Line 3.0 and the Voice Gateway Media Card on the Succession Communication Server for Enterprise (CSE) 1000 Release 2.0 systems using CSE 1000 Element Management.

Element Management administration procedures

This section describes the administration procedures that can be performed using Element Management.

Turning off browser caching

Internet Explorer caching interferes with the Element Management application, in that users cannot see real-time changes as they occur. For this reason, Nortel Networks recommends that Internet Explorer's caching be turned off prior to using Element Management.

Follow the steps outlined in Procedure 32 on page 333 to prevent caching of Web pages by the Internet Explorer browser.

IP Line Operational Measurement report scheduling and generation

Operational Measurement (OM) reports provide important statistical and traffic information and feedback to the system administrator to better engineer the system. The information stored in the OM file applies only to the calls routed over the IP network by way of IP Line. OM reports give a quantitative view of system performance, such as jitter.

You can view a single Voice Gateway Media Card's Operational Measurements file directly from Element Management. This OM report is a view of the TPS and Voice Gateway channel activity on that single card. Use this procedure to view the individual information in each Voice Gateway Media Card in the node.

The Voice Gateway Media Card Operational Measurements (OM) file contains the following information:

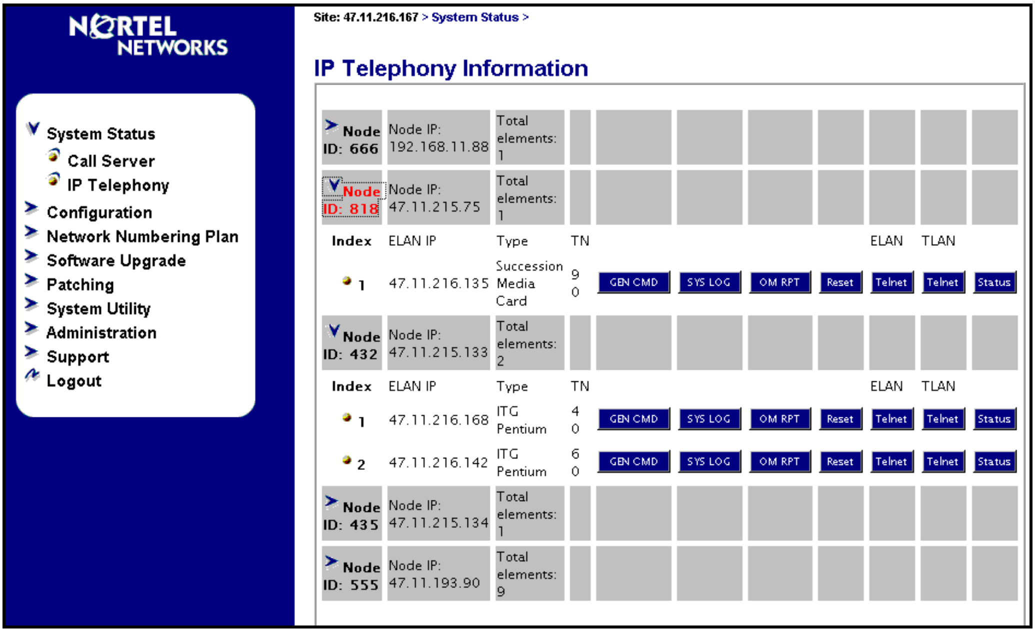
- the number of incoming and outgoing calls
- the number of call attempts
- the number of calls completed
- the total holding time for voice calls

To view a single Voice Gateway Media Card's Operational Measurements file directly from Element Management, follow the steps in Procedure 75 on page 500.

Procedure 75
Retrieving the current OM file from the Voice Gateway Media Card using Element Management

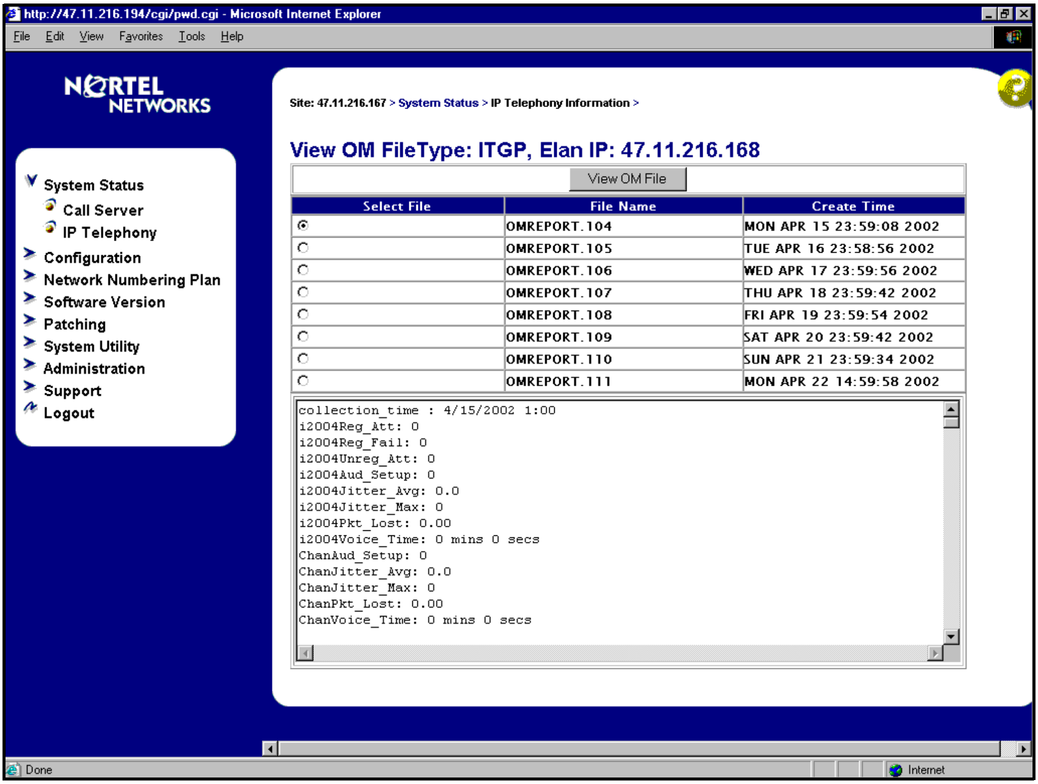
1. Click **System Status** in the Navigation Tree.
2. Click **IP Telephony**. The **IP Telephony Information** page opens.
3. Expand the node containing the Voice Gateway Media Card (see Figure 122 on page 500).

Figure 122
System Status > IP Telephony > IP Telephony Information



4 Click the **OM RPT** button associated with the Voice Gateway Media Card. The **View OM File** page opens (see Figure 123 on page 501).

Figure 123
System Status > IP Telephony > IP Telephony Information > View OM File



5 The eight most recent OM Report files are displayed in chronological order for the Voice Gateway Media Card.

To view a OM file, click the radio button for the file to be viewed and then click the **View OM File** button. The OM report data appears at the bottom of the page.

The file contains collection period information for each hour of the day that the card was running.

The collection periods start with the hour from midnight to 1:00am. As each hour passes, a collection period is added to the OM file. So there is a maximum of 24 collection periods each day.

A collection period looks like the following:

collection_time : 2/8/2002 9:00
i2004Reg_Att: 1
i2004Reg_Fail: 0
i2004Unreg_Att: 0
i2004Aud_Setup: 1
i2004Jitter_Avg: 0.1
i2004Jitter_Max: 0
i2004Pkt_Lost: 0.00
i2004Voice_Time: 0 mins 2 secs
ChanAud_Setup: 1
ChanJitter_Avg: 6.0
ChanJitter_Max: 20
ChanPkt_Lost: 0.00
ChanVoice_Time: 0 mins 2 secs
Note: During this collection period, reboot(s) occurred.

Each collection period provides the following:

- The date and time for the collection period hour.
- TPS information for Internet Telephones that are registered to the TPS on the Voice Gateway Media Card during that hour. The TPS information is prefixed by *i2004*. During normal operation, the TPS values for the Voice Gateway Media Card can be zeros as the Internet Telephone normally register to the TPS on the Signaling Server.
- Voice Gateway channel information accumulated during the hour. The Voice Gateway data is prefixed by *Chan.*
- Notes indicating whether the machine has been rebooted during the hour.
- Virtual Trunk statistics display only for a Signaling Server that has been running the VTRK H323 Signaling Server in the last hour.

The OM file relates to the omreport.xxx file on the Voice Gateway Media Card, where xxx indicates the numbers of days since December 31.

In general, there is no relationship between the Internet Telephones registered on a card and the Voice Gateway channels on the card (if there are two or more cards) in the node. If there is only one card (with multiple Internet Telephones), there may be a partial correlation between the Internet Telephones and the card information. However, even with only one card there still is not a 100% correlation, since an Internet Telephone can still call another Internet Telephone without involving the Voice Gateway channels.

End of Procedure

Note: Element Management supports the ability to view OM files only. OTM can optionally be used to support other Operational Measurements tasks such as scheduling reports, generating reports, opening reports, and viewing reports. See page 451 for more information.

Viewing IP Line log files

Element Management uses RPC to transfer the sysfile from the Voice Gateway Media Card to the PC. The error log file displays error information, including error date/time, the originating module (IP Telephony node), and specific error data.

To view error conditions that are abnormal events, but not severe enough to raise an alarm, follow the steps in Procedure 76 on page 504:

Procedure 76
Viewing IP Line log files

1 Click **System Status** in the Navigation Tree.

2 Click **IP Telephony**. The **IP Telephony Information** page appears.

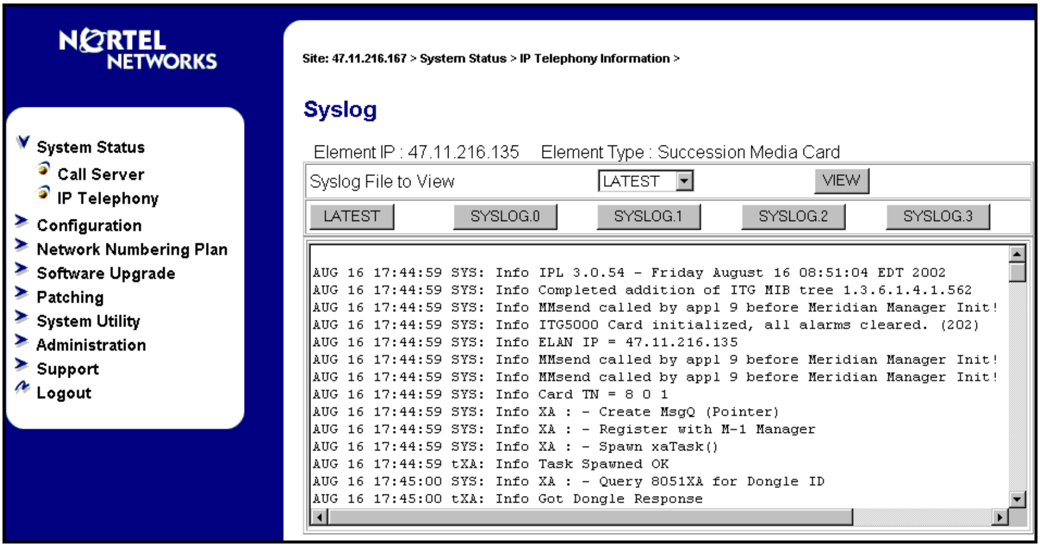
3 Expand the node containing the Voice Gateway Media Card (see Figure 122 on page 500).

4 Click the **SYS LOG** button associated with the Voice Gateway Media Card. The **Syslog** page appears (see Figure 124 on page 505).

5 The Syslog page has five buttons to view the log files:

- The LATEST button displays the most recent syslog information for the Voice Gateway Media Card.
- There are four SYSLOG.# buttons; one for each of the four syslog files on the Voice Gateway Media Card.

Figure 124
System Status > IP Telephony > Syslog



6 Click the LATEST button to view the most current syslog information that was written to the Voice Gateway Media card, or click the SYSLOG.0-3 buttons to view any of the syslog files.

The syslog file data is displayed in the window below the buttons. The data can be error messages or information messages. For each message, the date, timestamp, and the task that is printing the message is displayed.

End of Procedure

Backup and restore data

All data is stored on the Call Server. Element Management accesses the data for the elements being maintained. Element Management does not store data.

There is no Element Management specific data that needs to be backed up. All data is retrieved from the Call Server and elements.

The c:/u/db/node directory is populated on the Call Server when the node configuration is saved. The BOOTP.TAB and CONFIG.INI files are saved in this directory as c:/u/db/node/nodexxxx.btp and c:/u/db/node/nodexxxx.cfg where xxxx is the node ID:

- nodexxxx.btp is the BOOTP.TAB file
- nodexxxx.cfg is the CONFIG.INI.

If a node is removed, the associated files are also removed. For every node that is created, nodeyyyy.btp and nodeyyyy.cfg file are created in the C:/u/db/node directory.

WARNING
Do not manually edit or delete the node files. Manually editing or deleting these files can cause corruption of Element Management.

Backup

The Backup command invokes the Equipment Data Dump (EDD) operation on the Call Server to backup all Call Server data. Within Element Management, the **Call Server Backup** function invokes a data dump and writes the Call Server data to the primary and internal backup drives.

The backup includes all Call Server data as well as the BOOTP.TAB and Config.ini files for each node configured in the system. These files are stored on the Call Server for the IP Telephony nodes configured in the Succession CSE 1000 system.

This Backup function can also be done on the Call Server by entering the **EDD** CLI command through LD 43.

During the Backup function, the BOOTP.TAB and CONFIG.INI files of all registered nodes are copied so they can be restored in case of system failure.

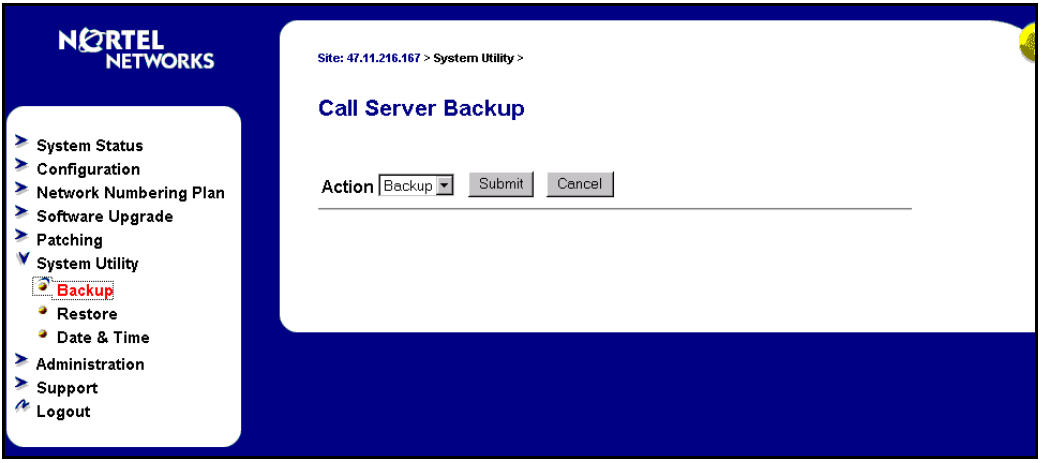
Follow the steps in Procedure 77 on page 507 to backup the Call Server.

Procedure 77
Backing up the Call Server data

1 Click **System Utility** in the Navigation Tree.

2 Click **Backup**. The **Call Server Backup** page opens (see Figure 125 on page 508).

Figure 125
System Utility > Backup

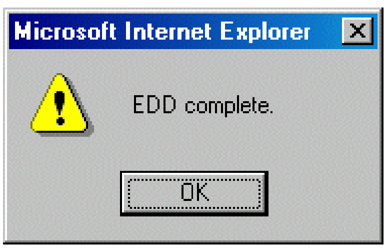


3 Select **Backup** from the Action drop-down listbox.

4 Click the **Submit** button. The page displays messages indicating that the “Backup in progress. Please wait...”

5 Click OK in the EDD complete dialog box (see Figure 126 on page 508).

Figure 126
EDD complete



The Backup function then displays information in a tabular form indicating the actions that were performed.

End of Procedure

Restore

The **Call Server Restore** function restores the backed up files from the internal backup device to the primary device. The Restore function performs the same task as the **RIB** CLI command in LD 43.

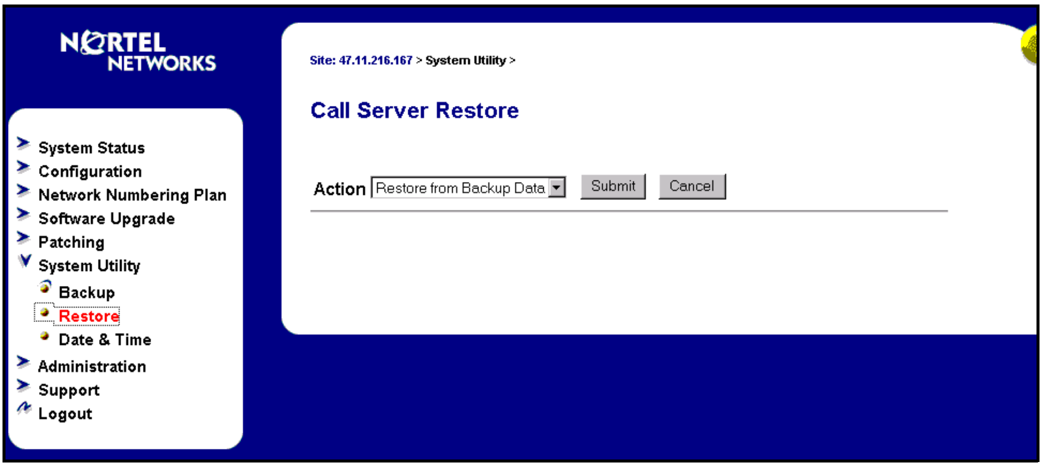
To restore the Call Server data, follow the steps in Procedure 78 on page 509.

Procedure 78
Restoring the Call Server data

1 Click **System Utility** in the Navigation Tree.

2 Click **Restore**. The **Call Server Restore** page opens (see Figure 127 on page 509).

Figure 127
System Utility > Restore



3 Select **Restore from Backup Data** from the Action drop-down listbox.

4 Click the **Submit** button.

If the Restore is successful, the message “Restore was done successfully” is displayed.

End of Procedure

Update IP Telephony node properties

To update the node properties of a Voice Gateway Media Card, follow the steps in Procedure 79.

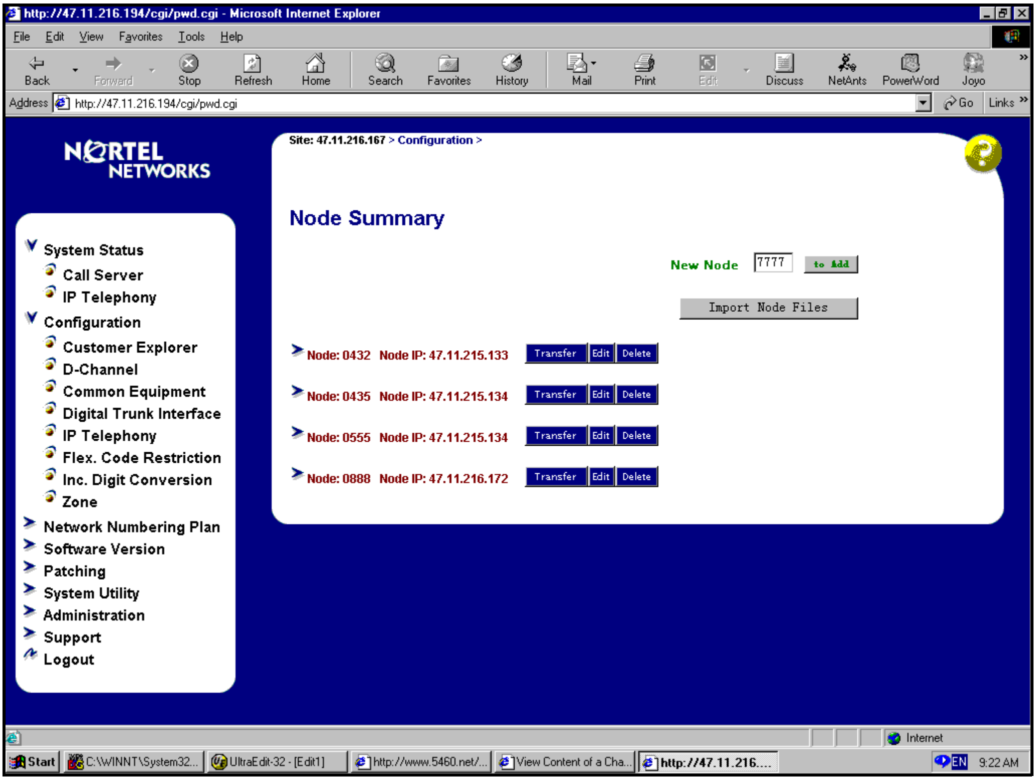
Procedure 79
Updating the IP Telephony node properties

1 Click **Configuration** in the Navigation Tree.

2 In the Configuration menu, click **IP Telephony**. The **Node Summary** page opens.

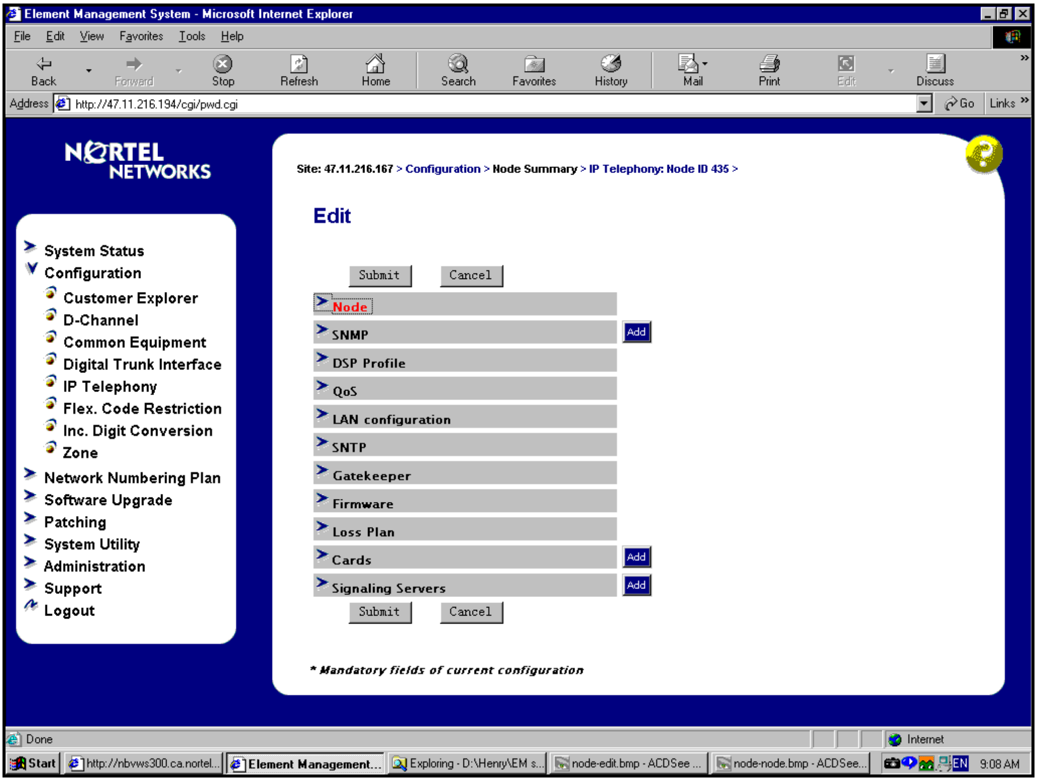
3 Click the **Edit** button associated with the node to be updated (see Figure 128 on page 511).

Figure 128
Element Management–Node Summary



4 The **Edit** page opens (see Figure 129 on page 512).

Figure 129
Element Management–Edit



5 Perform all required updates to the parameters in the appropriate sections.

6 If you add, delete, or replace Voice Gateway Media Cards from the node or change a Voice Gateway Media Card (refer to the Maintenance section for the procedure to replace a Voice Gateway Media Card), then use one of the following procedures:

- “Adding a Voice Gateway Media Card to the node” on page 513
- “Deleting a Follower Voice Gateway Media Card from the node” on page 522
- “Changing the IP addresses of an IP Telephony node in Element Management” on page 525
- “Replacing a Follower Voice Gateway Media Card” on page 614

End of Procedure

Adding a Voice Gateway Media Card to the node

To add a Voice Gateway Media Card to the node, follow the steps in Procedure 80.

Procedure 80
Adding a Voice Gateway Media Card to the node

1 Choose a card slot for the new card. Note the TN.

2 Configure IPTN in LD 14 at the Call Server.

3 Install the I/O cables for connection to the ELAN and TLAN on the selected card slot.

4 Click **Configuration** in the Navigation Tree.

5 In the Configuration menu, click **IP Telephony**. The **Node Summary** page opens.

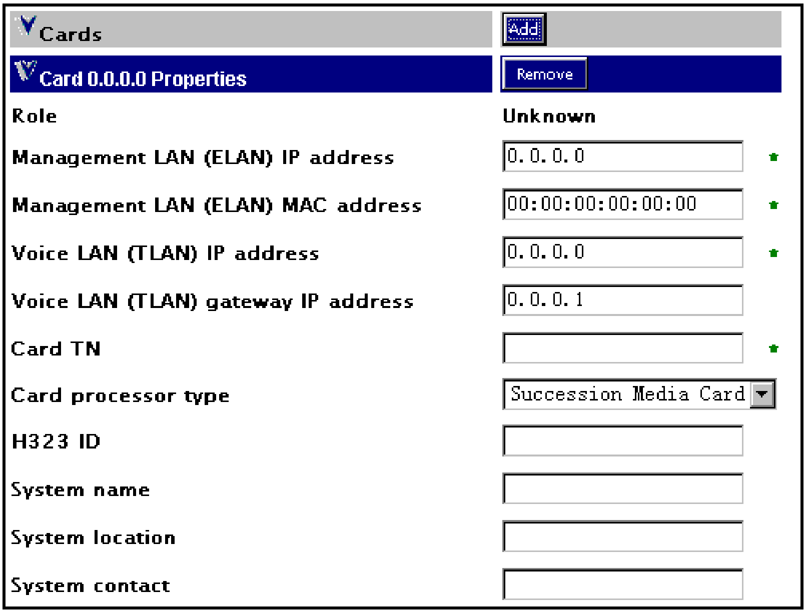
6 Click the **Edit** button for the node that is receiving the new Voice Gateway Media Card. The **Edit** page opens.

7 Click the **Add** button to the right of the Cards section (see Figure 130 on page 514).

Figure 130
Cards–Add button

8 Observe that the Cards section expands (see Figure 131 on page 514).

Figure 131
Configuration > Node Summary > Edit > Add Card



9 Enter the **Card Properties** data:

a. **Role:** Element Management reads the role form the card configuration.

b. **Management LAN (ELAN) IP address:** This is the ELAN IP address for the card. Element Management and Succession CSE 1000 use this address to communicate with the card.

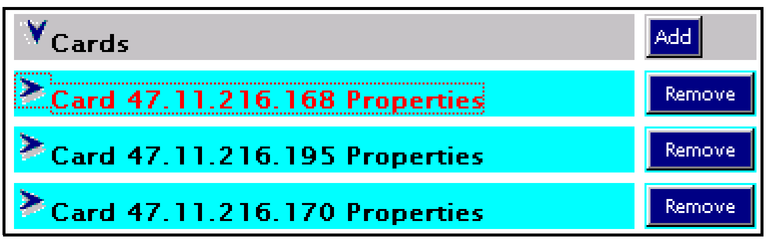
c. **Management LAN (ELAN) MAC address:** This is the motherboard Ethernet address from the “Voice Gateway Media Card installation summary sheet” on page 209.

- **d.** **Voice LAN IP (TLAN) address:** This is the TLAN IP address for the card.
- **e.** **Voice LAN gateway (TLAN) IP address:** This is the IP address of the router interface on the TLAN.
- **f.** **Card TN:** Enter the card slot number between 1-50.
- **g.** **Card processor type:** Choose either Pentium or Succession Media Card. Select Pentium if using the ITG-P Line Card (dual-slot card), or select Succession Media Card if using MC (single-slot card).
- **h.** **H323 ID:** The H323 ID within IP Line is for the Virtual Office/Branch Office feature. Keep the H323 ID the same for all the elements within one node.
- **i.** **System name:** Enter the name of the system.
- **j.** **System location:** Enter the location where the system resides.
- **k.** **System contact:** Enter the system contact name and phone number.

10 To add additional cards to the node, click the **Add** button again and enter the new card information. Repeat this step for each card to be added to the node.

11 Observe that new cards appear under the Cards section as they are added (see Figure 132 on page 515).

Figure 132
Cards



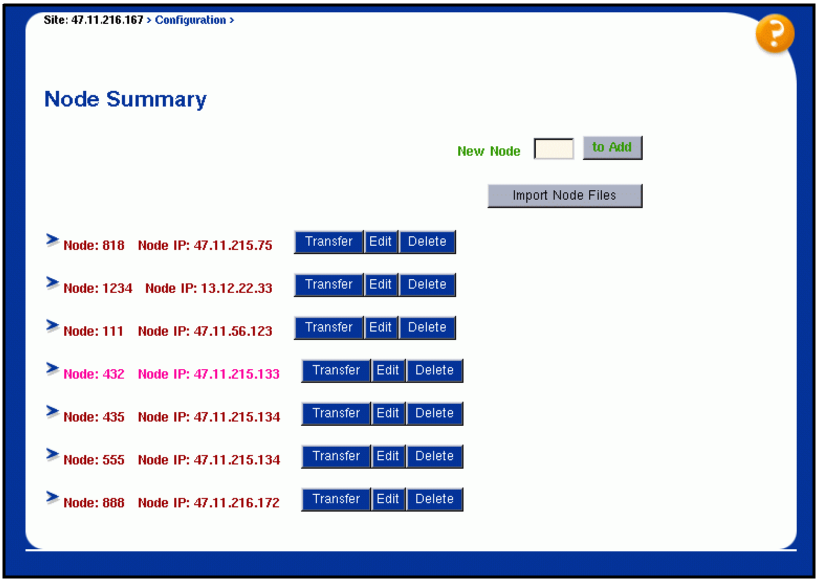
12 Click the **Submit** button after the card(s) has been added and configured. Clicking the **Submit** button saves the data to the Call Server. Click **OK** to confirm.

Note 1: The Submit button can be clicked after each card is configured in the Edit page. However, each time the Submit button is clicked, the Edit page closes and the Node Summary page is displayed. To continue the node configuration, click the Edit button to return to the Edit page.

Note 2: If the Cancel button is clicked, all information that has been configured is discarded. The Edit page closes and the Node Summary page opens.

13 The Edit page closes, and the Node Summary page opens (see Figure 133 on page 516).

Figure 133
Node added to Node Summary page



14 Click the **Transfer** button associated with the node where the new card(s) was added.

15 Click **OK** to confirm the transfer (see Figure 134 on page 517).

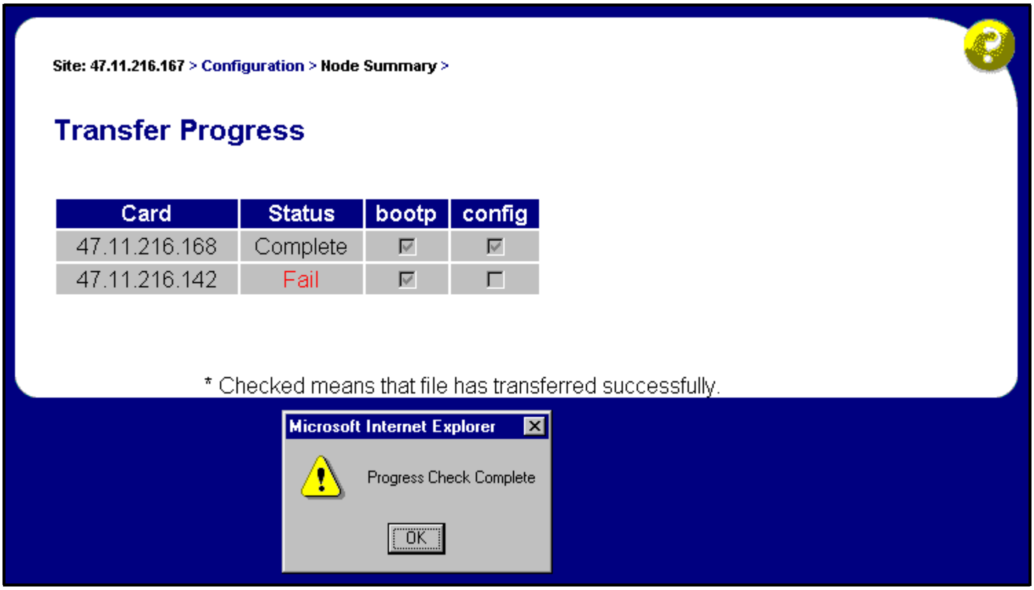
Figure 134
Transfer confirmation dialog box

16 The **Transfer Progress** page opens and displays each of the Voice Gateway Media Card in the node (see Figure 135 on page 518).

The Voice Gateway Media Card's retrieve the CONFIG.INI and BOOTP.TAB files from the Call Server. A check mark is added to each field as the card receives its CONFIG.INI and BOOTP.TAB files. When the transfer is complete, click **OK** in the Progress Check Complete dialog box.

- If the transfer is successful for a card, the Status column displays "Complete".
- If the transfer is unsuccessful, the Status column displays "Fail".

Figure 135
Transfer Progress page



17 Insert the new card. The card starts and obtains its IP configuration from the node master. This takes several minutes.

The Maintenance faceplate display shows an alarm of T:21 or S009.

- T:21 is displayed if the card is new and there is no CONFIG.INI file.
- S009 can be displayed if the card has been used before and has a CONFIG.INI file that contains an IP address for the Call Server that is no longer correct.

18 Select **System Status | IP Telephony** from the Navigation Tree. The IP Telephony Information pages appears. Expand the node containing the Voice Gateway Media Card.

19 Click the **GEN CMD** button associated with the Voice Gateway Media Card. The **General Commands** page opens. Click the **cardRoleShow** command from the drop-down list box.

If the card role is not follower as expected, telnet to the card's IPL> CLI and enter the clearLeader command to remove the clearLeader flag.

20 In the **Node Summary** page of the Element Management application, click the **Transfer** button. This downloads the node information to the card.

21 Click **System Status** in the Navigation Tree. Click **IP Telephony**. The IP Telephony Information page appears.

22 Expand the node containing the new card(s) that were added.

23 Click the **Status** button for each Voice Gateway Media Card that was added.

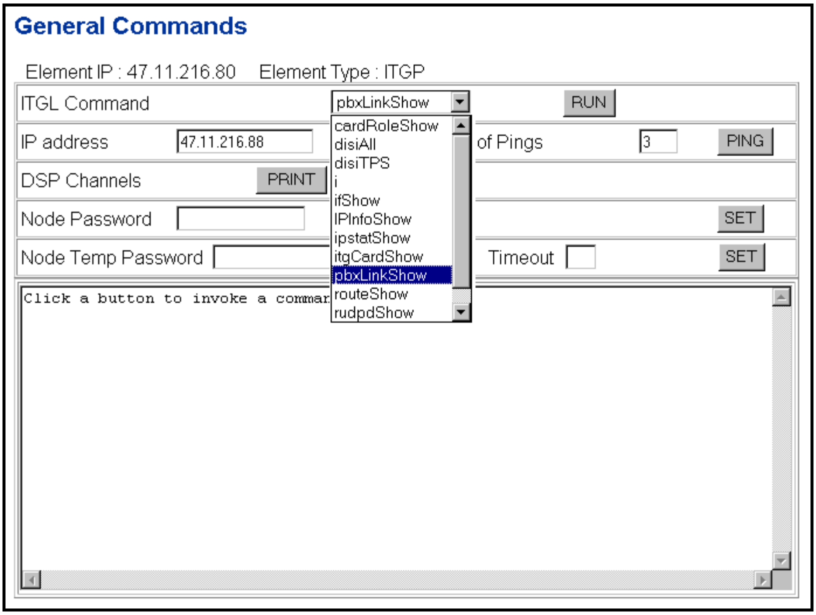
The card status should display as “Enabled” or "Disabled". If the status message of “WEB3003: Destination IP address cannot be reached; initial RPC failure” is displayed, then verify the network connection and the proper configuration of the network equipment.

24 Verify that all the new Voice Gateway Media Cards in the node have a signaling link to the Call Server.

25 Click **System Status | IP Telephony Information**. Go to the **General Command** page. Click the **pbxLinkShow** command from the drop-down list box (see Figure 136 on page 520).

Alternatively, telnet to each Voice Gateway Media Card and log in. Enter the pbxLinkShow CLI command at the IPL> prompt.

Figure 136
General Commands > pbxLinkShow



Note: The **pbxLinkShow** command can also be entered at the IPL> command line or you can also look at the display on the card's faceplate and ensure it is not displaying an alarm.

The pbxLinkShow command output is similar to the following:

Active CS type = Succession CSE 1K
Active CS S/W Release = 201R
Supported Features: GetCSVsn TCP ShiftKey I2050 I2002 CorpDir UserKeyLabel VirtualOffice UseCSPwd
CS Main: ip = 47.104.39.112, ConnectID = 0x2bbfb4c, BroadcastID = 0x2bc059c, Link is up
CS Signaling Port = 15000
CS Broadcast Port = 15001
Broadcast PortID = 0x2bc06fc
RUDP portID = 0x2bc0684
Tcp Link state = up
Tcp Signaling Port: 15000
Tcp socket fd: 30
Tcp msgs sent: 77
Tcp msgs recd: 47

26 Select **System Status | IP Telephony** from the Navigation Tree. The IP Telephony Information pages appears. Expand the node containing the Voice Gateway Media Card.

27 Click the **GEN CMD** button associated with the Voice Gateway Media Card. The **General Commands** page opens. Click the **cardRoleShow** command from the drop-down list box.

If the card role is not Follower as expected, telnet to the card's IPL> CLI and enter the clearLeader command to remove the clearLeader flag.

28 Verify the card loadware and firmware version on the new card and, if necessary, upgrade the loadware and the firmware. Use the procedures outlined in the section "Upgrade the Voice Gateway Media Card loadware and Internet Telephone firmware" on page 377.

End of Procedure

Deleting a Follower Voice Gateway Media Card from the node

To delete a Voice Gateway Media Card from the node, follow the steps in Procedure 81.

Procedure 81
Deleting a follower Voice Gateway Media Card from the node

1 Click **Configuration** in the Navigation Tree.

2 In the Configuration menu, click **IP Telephony**. The **Node Summary** page appears.

3 Click the **Edit** button for the node containing the Voice Gateway Media Card to be deleted. The **Edit** page appears.

4 Expand the **Cards** section.

5 Confirm the card to be deleted and then click the **Remove** button for that card (see Figure 137 on page 522).

Figure 137
Configuration > Node Summary > Edit > Remove Card

6 Click **Submit** and then click **OK** to save the node change.The Edit page closes, and the Node Summary page opens.

7 Click the **Transfer** button associated with the node containing the card that was removed. Click **OK** to confirm the transfer.

8 The Transfer Progress page opens and the changes are transferred to the Call Server. Click **OK** in the Progress Check Complete dialog box.

9 Remove the Voice Gateway Media Card.

CAUTION WITH ESDS DEVICES
Follow the anti-static procedures and place the Voice Gateway Media Card in an appropriate anti-static package.

10 Remove the Voice Gateway Media Card configuration data from the Call Server.

a. Identify the TN of the Voice Gateway Media Card.

b. In LD 20, enter the **LTN** (List Terminal Number) command where TYPE = tie, to list the TNs on the Voice Gateway Media Card TN. This returns a list of units equipped on the card. Verify the number of units that are equipped on the card. Note the first unit equipped on the card.

c. In LD 14, use the **Out n** command, where **n** equals the number of units that are equipped on the card.

11 At the TN prompt, enter the TN for the first unit that was equipped on the card. As the units are deleted, verify that you have "outed" the intended units.

End of Procedure

Deleting the Leader Voice Gateway Media Card from the node

In the normal Succession CSE 1000 Rel 2.0 system, the Signaling Server is the Leader of the node. However, if a second or subsequent node is configured on the system, then a Voice Gateway Media Card is configured as the Leader for that node. If a user deletes the Leader card for a second or subsequent node (that is, the card in Element Management that displays the card role as Leader), then another card in the node must be selected and the setLeader command must be issued on that card. A node must have a Leader card for it to operate correctly on power up of the node.

> ***Note:*** The role of a card can be viewed in Element Management, it cannot be changed. The Element Management GUI displays the card role based on the setLeader status of the card.

Follow the steps in the Procedure 82 on page 524 to first select a new Leader card and then to delete the current Leader Voice Gateway Media Card.

Procedure 82
Deleting the Leader Voice Gateway Media Card

1. Click **System Status** in the Navigation Tree and then click **IP Telephony**.
2. In the IP Telephony Information page, expand the node containing both the Leader card to be deleted and the card that will become the new Leader.
3. Select a card in the node to become the new Leader (Card A).
4. Click the **Telnet** button to the right of the Card A and log in to the card.
5. Enter the **setLeader** command. Card A becomes the new Leader.
6. In the IP Telephony Information page, expand the node containing the “old” Leader card (Card B) which is to be deleted.
7. Click the **Telnet** button to the right of the Card B and log in to the card.
8. Enter the **clearLeader** command. This command removes the IP address information from NVRAM and also clears the Leader flag.
9. Remove the “old” Leader card (Card B) from the Media Gateway.
10. Reboot Card A. Wait for the card to come up as the Leader.
11. Click **Configuration** and then **IP Telephony**.
12. On the Node Summary page, click **Edit** for the node.
13. On the **Edit** page, click the **Remove** button for the “old” Leader card (Card B) that was remove.
14. Click **OK** to confirm the deletion of the card.
15. Click **Submit**.
16. In the **Node Summary** page, click the **Transfer** button associate with the node containing the new Leader card and the deleted Leader card.

End of Procedure

Changing the IP addresses of an IP Telephony node in Element Management

Prior to changing any IP address, ensure you understand the "IP Network Engineering Guidelines" on page 133, and consult with the IP network administrator.

IP address configuration changes are completed in four sections of the Edit Page. The four sections are:

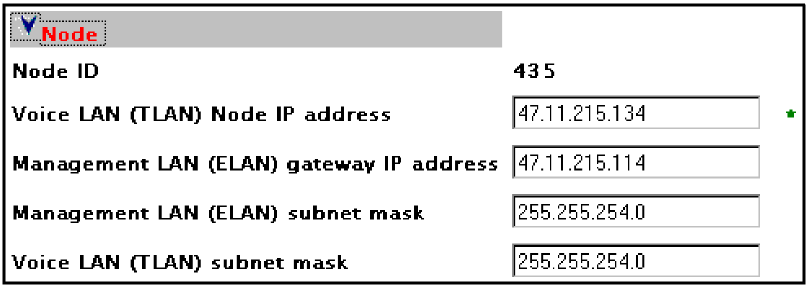
- Node – Configure network connections in this section.
  See Figure 138 on page 526.
- Card – Card properties are set in this section.
  See Figure 139 on page 528.
- SNMP– SMNP traps are enabled and configured in this section
  See Figure 140 on page 530.
- LAN Configuration– ELAN/TLAN settings and card routing table entries are configured in this section.
  See Figure 141 on page 531.

To change the IP address of an IP Telephony node, follow the steps in Procedure 83 on page 525.

Procedure 83
Changing the IP addresses of an IP Telephony node in Element Management

1. Click **Configuration** in the Navigation Tree.
2. In the Configuration menu, click **IP Telephony**. The **Node Summary** page appears.
3. Click the **Edit** button for the node that is having the IP address changes. The **Edit** page appears.
4. Expand the **Node** section, if it is not already expanded (see Figure 138 on page 526).

Figure 138
Node Properties



a. **Node ID:** The Node ID appears automatically.

b. **Voice LAN (TLAN) Node IP address:** Enter Voice LAN (TLAN) Node IP address in dotted decimal format. The Voice LAN Node IP is on the TLAN. The Node IP address is the IP address used by the Internet Telephones to communicate with the Voice Gateway Media Cards on the TLAN. If a Voice Gateway Media Card becomes the primary (Leader) during an election, it assigns itself the Node IP address.

- If the node IP is changed, this affects the configuration of the Connect Server IP address in the DHCP Server for the Internet Telephones.
- If the Internet Telephones are using partial DHCP mode, manually reconfigure the IP address of each Internet Telephone.

c. **Management LAN (TLAN) gateway IP address:** Enter Management LAN (ELAN) gateway IP address in dotted decimal format. This is the IP address of the gateway of the subnet to which the Voice Gateway Media Card belongs. This is the IP address of the router interface on the ELAN, if present. If there is no management LAN gateway, enter 0.0.0.0.

- When a Management LAN gateway is added to the ELAN, it must restrict access so that only authorized traffic is permitted on the ELAN.
- The router must disable the BootP relay agent for ELAN interface.
- The router must block all broadcast and multicast traffic from the ELAN and enable only proper access, that is, only authorized traffic and users coming through the Management LAN gateway.

d. **Management LAN (ELAN) subnet mask:** Enter the Management LAN subnet mask address in dotted decimal format. This is the subnet mask that is used along with the ELAN IP address to identify which subnet the Voice Gateway Media Card belongs. When changing these subnet masks, consider the possibility of conflict between the ELAN and TLAN IP addresses. Consult with the IP administrator before making any changes to subnets. Refer to "IP Network Engineering Guidelines" on page 133.

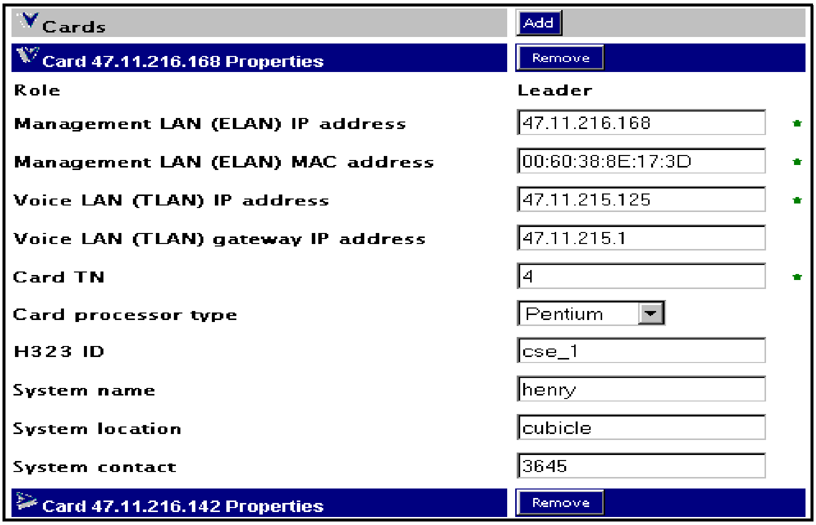
When changing the Management LAN (ELAN) subnet, this must be coordinated with the IP address on the Call Server (Active ELNK) subnet. You must also coordinate changes with the following:

- Management LAN gateway, and other IP devices on the ELAN
- any other devices on the ELAN and customer's enterprise network (CLAN) that need to communicate with IP Line
- devices that are looking to receive SNMP traps

e. **Voice LAN (ELAN) subnet mask:** Enter the Voice LAN subnet mask address in dotted decimal format. This is the subnet mask that is used along with the TLAN IP address, to identify the subnet to which the Voice Gateway Media Card belongs. Coordinate with Voice LAN gateway (router). When changing the Voice LAN (TLAN) subnet mask, the change must be coordinated with changing the subnet mask of the Voice LAN (TLAN) gateway (router) interface.

5 Expand the **Cards** section and select the card to be changed (see Figure 139 on page 528).

Figure 139
Cards



6 Enter the **Card Properties** data for the Leader and Follower cards:

a. **Role:** The first card in the node must exist. This card is the Leader. Every IP Telephony node must have only one Leader. All other cards function as Followers. This field is read-only.

b. **Management LAN (ELAN) IP address:** This is the ELAN IP address for the card. Element Management and Succession CSE 1000 use this address to communicate with the card.

   If you are changing the Management LAN IP address of the Leader card, you must Telnet to the card and use the setLeader command to make the same change (new Management IP address) in the NVRAM of the Leader card.

   The Leader must be reset to resume communication with the node.

Note: Prior to resetting the Leader, unplug all the other cards to prevent any other card from becoming the Master. When the Leader restarts, plug the cards back in. These other cards receive their new configuration from Leader 0.

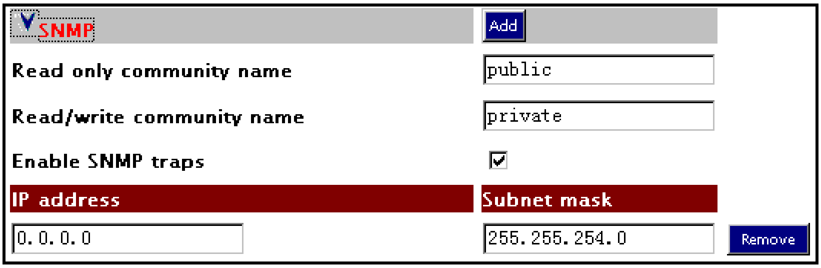
c. **Management LAN (ELAN) MAC address:** This is the motherboard Ethernet address from the "Voice Gateway Media Card installation summary sheet" on page 209. All other IP configuration depends on the accurate configuration of the Management MAC address. The MAC address is located on the faceplate of the Voice Gateway Media Card and is labelled as MOTHERBOARD Ethernet address. The Management MAC address corresponds to the ELAN address.

d. **Voice LAN (TLAN) IP address:** This is the card voice IP address. This address is also known as the card TLAN IP address. In an IP Telephony node, all cards must be assigned an address on the same TLAN subnet. The card voice IP address must be distinct from the node IP address.

e. **Voice LAN (TLAN) gateway IP address:** This is the IP address of the router interface on the TLAN. All cards in the IP Telephony node must be on the TLAN; therefore, they all share the same Voice LAN / TLAN gateway IP address.

7 Click **SNMP** (see Figure 140 on page 530).

Figure 140
SNMP



a. **Read only community name:** Leave the default selection.

b. **Read/write community name:** Leave the default selection.

c. **Enable SNMP traps:** Check the Enable SNMP traps checkbox, if configuring one or more SNMP management IP addresses to receive SNMP traps from cards in the IP Telephony node.

d. **IP address:** If SNMP traps are enabled, the SNMP traps are sent to the IP address entered here.

e. **Subnet mask:** If SNMP traps are enabled, this is the subnet mask of where SNMP traps are sent.

IP addresses that are added here create special card routing tables that direct packets out the ELAN and ELAN gateway. Exercise caution when adding entries since the entry could result in one-way voice transmission if a change results in voice packets being streamed out the ELAN instead of the TLAN interface.

To add an SNMP Manager IP address, type the IP address in the SNMP traps entry fields, and click **Add**. Add SNMP Manager IP addresses for:

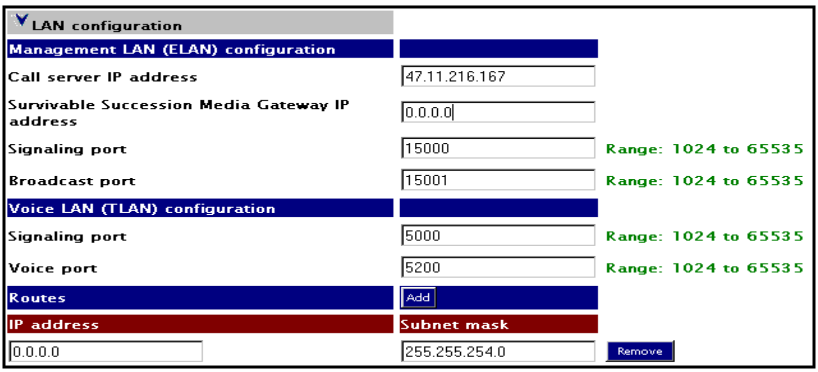
- the local or remote OTM server
- PPP IP address configured in the Netgear RM356 Modem Router, or equivalent, on the ELAN for the remote support OTM PC
- the SNMP manager for remote alarm monitoring

Note: A net route or host route through the management gateway is added to the Voice Gateway Media Cards IP Routing Table for each SNMP management address that is added to the SNMP traps list.

Changes can be made to the SNMP Traps without affecting other IP addresses. Change the SNMP traps as required, based on the destination host you are trying to reach.

8 Expand the **LAN Configuration** section (see figure Figure 141 on page 531).

Figure 141
LAN configuration



9 Enter the following **Management LAN (ELAN) configuration** settings:

a. **Call Server IP address:** This is the IP address of the Call Server on the Embedded LAN (ELAN). Enter the Call Server ELAN IP Address (Active ELNK).

Note: The Call Server ELAN IP address must correspond to the Active ELNK IP address configured in LD 117. It must be in the same subnet as the ELAN for the IP Line node.

b. **Survivable Succession Media Gateway IP address:** This is the IP address of the Survivable Succession Media Gateway on the ELAN.

Note 1: The Survivable Succession Media Gateway IP address must correspond to the Active ELNK IP address. If configured, all Voice Gateway Media Cards in the same node should be in the same Survivable Cabinet.

Note 2: The Survivable Media Gateway associated with the primary Signaling Server IP Telephony node is called the Alternate Call Server. It is usually located in the same equipment rack with the Call Server and Signaling Server. Therefore it is usually connected to the same ELAN subnet as the Call Server and the primary Signaling Server IP Telephony node. The Alternate Call Server Media Gateway is equipped with sufficient trunk cards and Voice Gateway Media Cards, and centralized Call Pilot in order to provide a large degree of survivability in case of Call Server equipment failure for Internet Telephone users who normally register through the Signaling Server.

Refer to *Installation and Configuration* (553-3023-210) for more information about survivability.

c. **Signaling port:** The default value is 15000. The range is 1024 to 65535.

d. **Broadcast port:** The default value is 15001. The range is 1024 to 65535.

10 Under **Voice LAN (TLAN) configuration**:

a. Signaling port: The default value is 5000. The range is 1024 to 65535.

Note: The TLAN Signaling occurs on UDP ports 7300, 4100, 5100, and 5000.

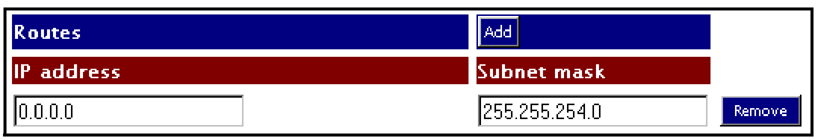
b. **Voice port**: Change the Voice port only as instructed by the IP network administrator to improve Quality of Service for the Internet Telephones. This field displays the range for RTP packets sent to the Internet Telephones. For example, if RTP Header compression is used to reduce voice bandwidth on narrow band WAN links, then the TLAN voice port range needs to be set to 16384 or higher.

The exact range is provided by the system administrator. In general, use the default value of 5200. If, however, there are numerous telephones working over low bandwidth WAN links using CISCO RTP header compression, then change the voice port to a number in the range of 16384 to 32767. Coordinate this value change with your IP network administrator.

Note: The TLAN Voice port range is 1024 to 65535. The default Voice ports are 5200 - 5295. A check is performed to prevent the TLAN Voice and signaling UDP ports from having the same range.

11 If entries must be made to the card routing table, click the **Add** button to the right of **Routes**. The Routes fields expand (see Figure 142 on page 533).

Figure 142
Routes



Under **Routes**, enter the I**P address** and **Subnet mask** for any host that is not on the ELAN subnet but requires access to the Voice Gateway Media Card across the ELAN. A Telnet session for maintenance from a remote PC is an example of when this would be needed. The address of the remote PC would be added in the Route list.

The default route on the card causes packets for unknown subnets to be sent out the TLAN interface. Packets from an external host arrive on the ELAN interface and responses are sent on the TLAN interface. This can cause one way communication if the TLAN is not routed to the ELAN. It is necessary to add an entry in the Route list to correct the routing so response packets are sent on the ELAN. Each entry creates a route entry in the card's route table that directs packets out the ELAN interface (see Figure 70 on page 357).

CAUTION
Use caution when assigning card routing table entries. Do not include the IP address of an Internet Telephone. Otherwise, voice traffic to these Internet Telephones is incorrectly routed through the ELAN and ELAN gateway. To avoid including the wrong IP address it is recommended that Host IDs are defined for the card routing table entries.

To add additional routes, click the **Add** button again and enter the route information. Repeat this step for each route to be added.

12 Click **Submit** and then click **OK**.

13 In the Node Summary page, click the **Transfer** button associated with the node that had the IP address changes.

End of Procedure

Restarting a Voice Gateway Media Card

If the IP address of a single card has changed, it must be restarted in order for the changes to take effect. However, if IP addresses that affect the entire node are changes, all cards in the node must be restarted.

Changes to the SNMP IP addresses take place immediately when the transfer occurs and restarting the cards are not required.

If the IP address of a Voice Gateway Media Card has changed, restart only that card using the step in Procedure 84 on page 535.

Procedure 84
Restarting a Voice Gateway Media Card

1 To prevent interruption to the speech path, login to LD 32.

2 Type the **DISI** command. This command disables the voice gateway channels when they become idle. DISI removes the call traffic but does not remove the Internet Telephones that are registered on that Voice Gateway Media Card. The Graceful TPS Disable command does this.

3 Type **disiTPS** at the card's IPL> prompt to disable the TPS service on the Voice Gateway Media Card. This Graceful TPS Disable command prevents new Internet Telephones from registering on the card. All Internet Telephones registered on the card are redirected to another Voice Gateway Media Card when the telephone becomes idle.

After the command is entered, an idle Internet Telephone should be updated with the Watchdog reset message. However, the TPS sends a soft reset message to the Internet Telephone, redirecting it to the Connect Server. The disabled TPS does not accept new registrations, so the Internet Telephones must register with another TPS in the node. Eventually, as all of the TPS's Internet Telephones become idle, they are registered with other TPSs. The Voice Gateway Media Card can then be removed with no impact to any users.

Alternatively, a Voice Gateway Media Card can be restarted from within Element Management.

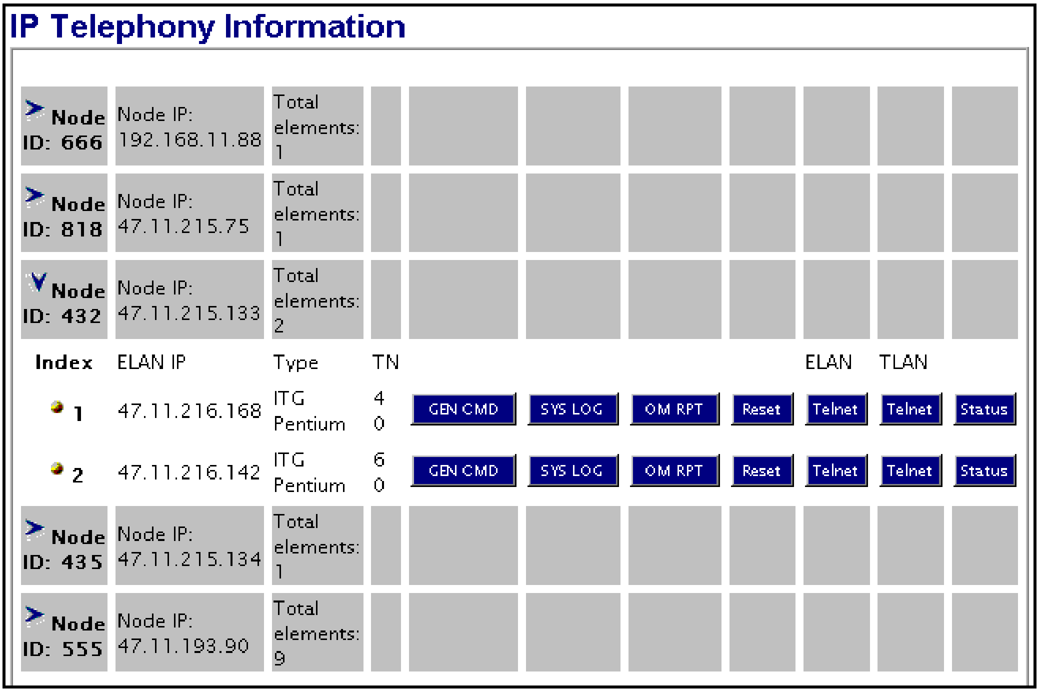
Procedure 85
Restarting a Voice Gateway Media Card

1 Click the **System Status** from the Navigation Tree. Click **IP Telephony**. The IP Telephony Information page opens.

2 Expand the node containing the Voice Gateway Media Card.

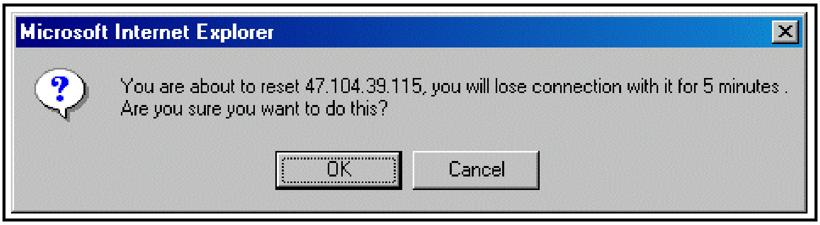
3 Click the **Reset** button associated with the Voice Gateway Media Card (see Figure 143 on page 536).

Figure 143
Reset button



4 Click **OK** to confirm the Voice Gateway Media Card reset (see Figure 144 on page 537).

Figure 144
Card Reset dialog box



End of Procedure

Restarting all the Voice Gateway Media Cards

All cards have to be restarted if there has been a change to the following:

- node IP address
- subnet of either the TLAN or ELAN (by changing the subnet mask or the subnet fields of the IP address)

These changes affect the whole node. As a result, all the cards have to be restarted.

If the Management IP address of the Leader has changed, all the cards have to be restarted. Even though this is a change to a single card, this change affects all cards, as this address is used to transmit properties to the node.

Procedure 86
Restarting all Voice Gateway Media Cards

1. Telnet to the card.
2. Use the **setLeader** command to set the new IP address. The Leader uses this new IP address when it reboots.
3. Reboot the Leader using the **cardReset** command. The Leader card reads the new IP address from NVRAM.
4. Restart all the other cards.

End of Procedure

Update other node properties

Some basic Voice Gateway Media Card configuration must be performed from the IP Telephony Node Edit page.

To update the node properties in the following sections:

- DSP Profile section, follow the steps in Procedure 36 on page 346
- QoS section, follow the steps in Procedure 37 on page 351
- Loss Plan section, follow the steps in Procedure 40 on page 360

Telnet to a Voice Gateway Media Card

To access the command line on a Voice Gateway Media Card from Element Management, perform Procedure 87 on page 538.

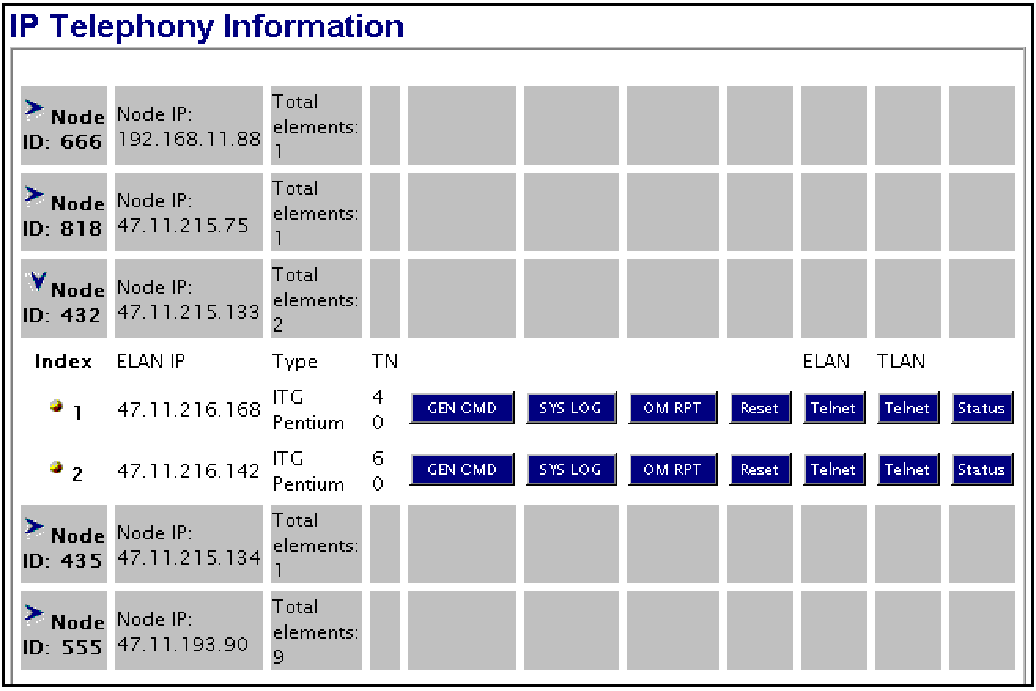
Procedure 87
Accessing a Voice Gateway Media Card using Telnet

1 Click the **System Status** from the Navigation Tree. Click **IP Telephony**. The IP Telephony Information page opens.

2 Expand the node containing the Voice Gateway Media Card.

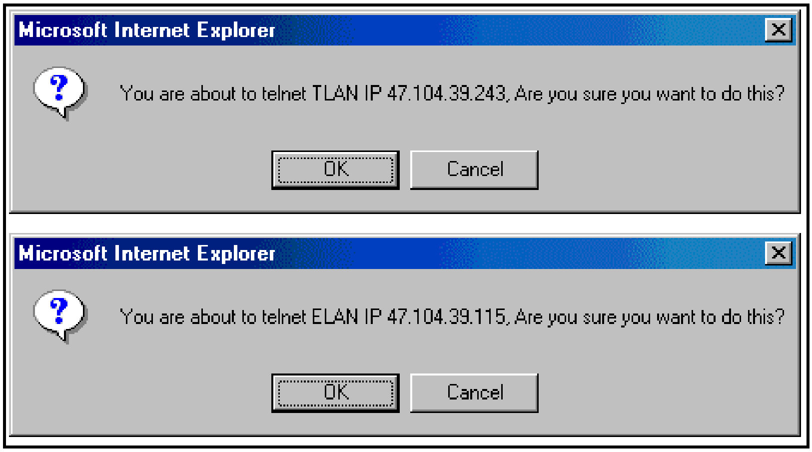
3 Click the **Telnet** button associated with the Voice Gateway Media Card (see Figure 145 on page 539).

Figure 145
Telnet



4 Click **OK** to confirm the Telnet session (see Figure 146 on page 540).

Figure 146
Telnet to ELAN or TLAN dialog boxes



5 A Telnet window opens and automatically connects to the Voice Gateway Media Card by using the TLAN or ELAN IP Address.

6 Enter a username and password to access the IPL> CLI.

Note: For Meridian 1 and Succession CSE 1000 Rel 1.1 systems, the default user name and password are both **itgadmin**. However, the user name and password should have been changed during installation. For Succession CSE 1000 Rel 2.0 systems, use the PWD1 userid and password.

7 The IPL> prompt appears if the login is successful. Type **?** at the prompt to display a list of available IPL> CLI commands. See “IP Line CLI commands” on page 567 for a detailed list of commands.

End of Procedure

Checking the Voice Gateway Channels

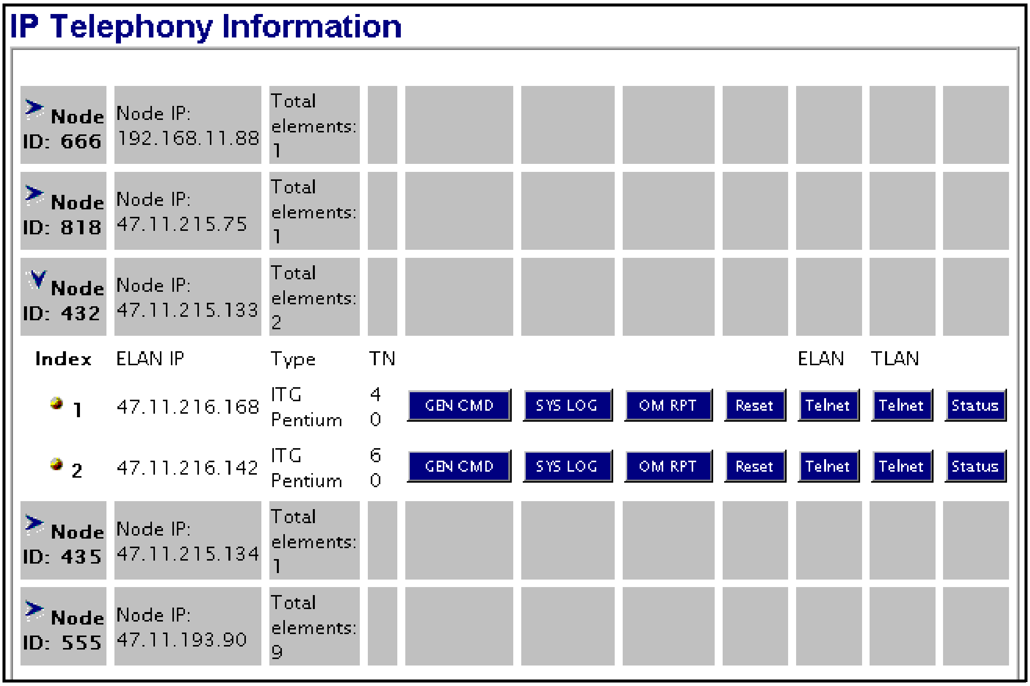
To check the Voice Gateway Channels running on a Voice Gateway Media Card, follow the steps in Procedure 88 on page 541.

Procedure 88
Checking the Voice Gateway Channels

1 Click **System Status**, and then **IP Telephony**. The IP Telephony Information page opens.

2 Expand the node to show all its elements (see Figure 147 on page 541).

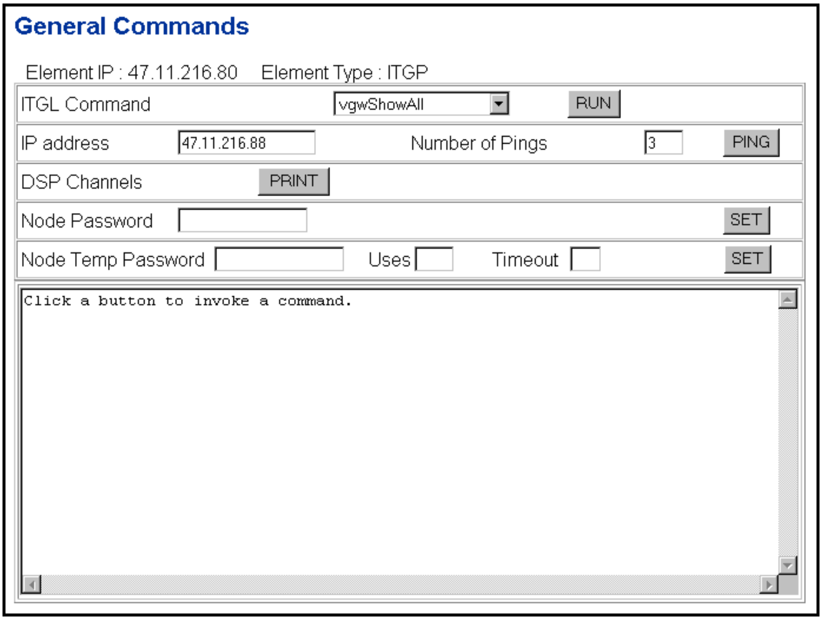
Figure 147
IP Telephony Information



3 Click the **GEN CMD** button associated with the Voice Gateway Media Card.

The **General Commands** pages opens (see Figure 148 on page 542).

Figure 148
General Command

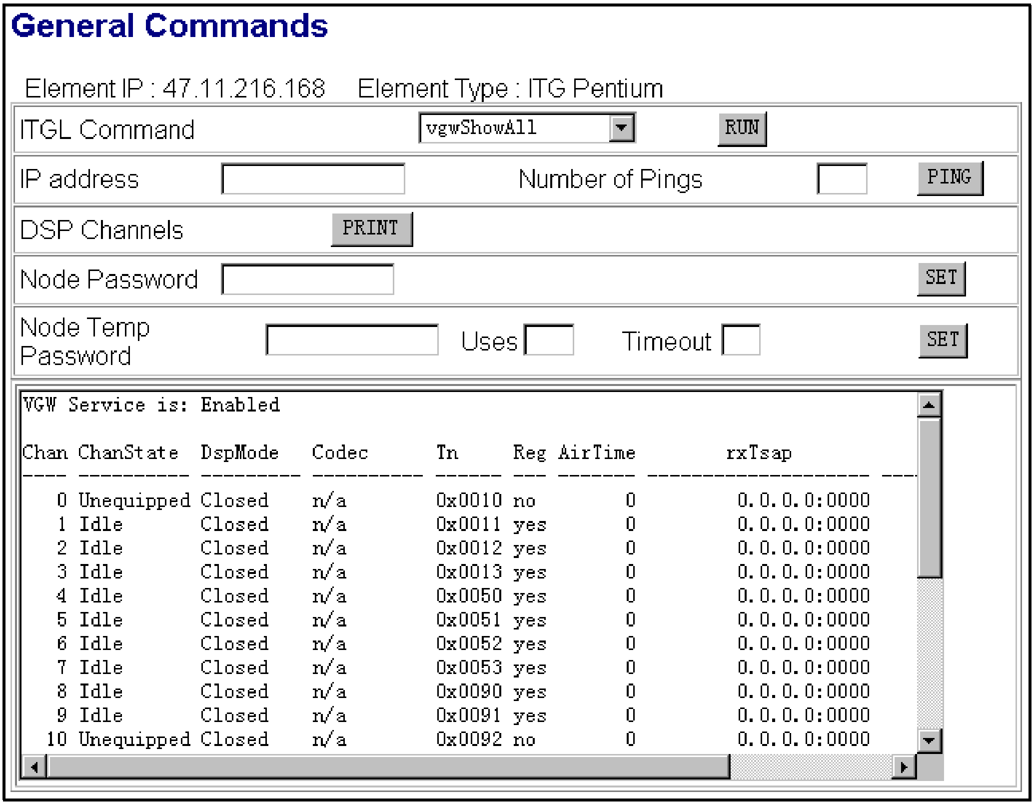


4 Select **vgwShowAll** from the ITGL Command drop-down list box.

5 Click **RUN**.

The output of the vgwShowAll command is displayed in the text area at the bottom of the page (see Figure 149 on page 543).

Figure 149
vgwShowAll output

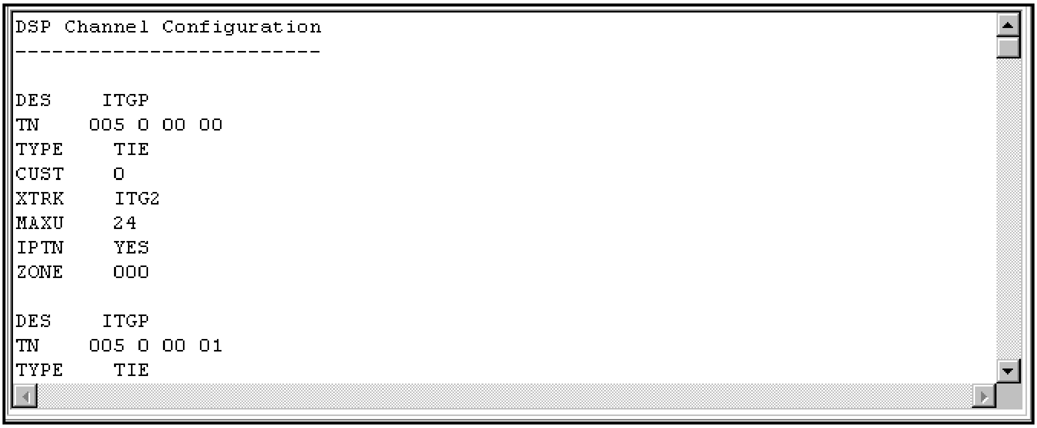


6 To view the DSP Channel configuration, go to the **DSP Channels** section of the General Commands page, and then click the **PRINT** button (see Figure 150 on page 543).

Figure 150
DSP Channels PRINT

The output of the DSP Channels PRINT command is shown in Figure 151 on page 544.

Figure 151
Output of DSP Channels PRINT



```
DSP Channel Configuration
-------------------------

DES     ITGP
TN     005 0 00 00
TYPE     TIE
CUST     0
XTRK     ITG2
MAXU     24
IPTN     YES
ZONE     000

DES     ITGP
TN     005 0 00 01
TYPE     TIE
```

End of Procedure

Setting the Internet Telephone Installer Password

Element Management includes the CLI commands for setting the administrative and temporary Internet Telephone Installer Password. For detailed information about the Internet Telephone Installer Password, refer to section “Internet Telephone Installer Password” on page 420.

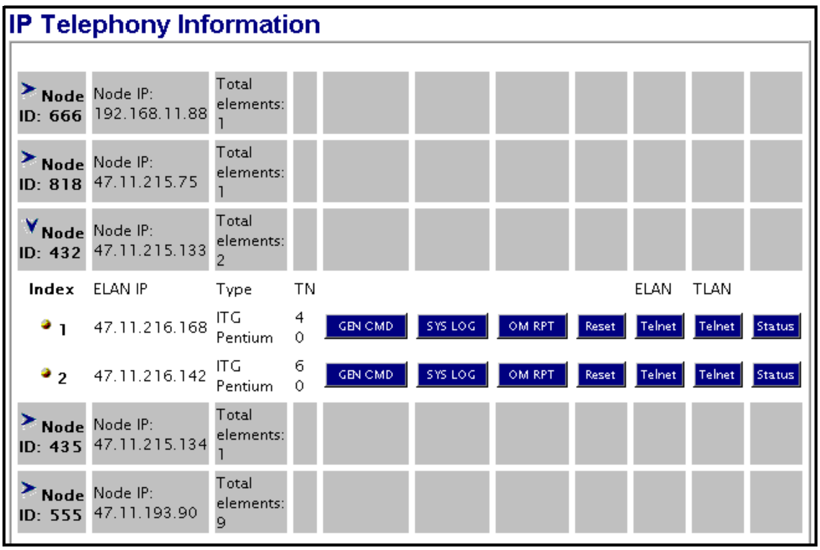
To set the Internet Telephone Installer Password in Element Management, follow the step in Procedure 89.

Procedure 89
Setting the administrative and temporary Internet Telephone Installer Passwords

1 Click **System Status**, and then **IP Telephony**. The IP Telephony Information page opens.

2 Expand the node to show all its elements (see Figure 152 on page 545).

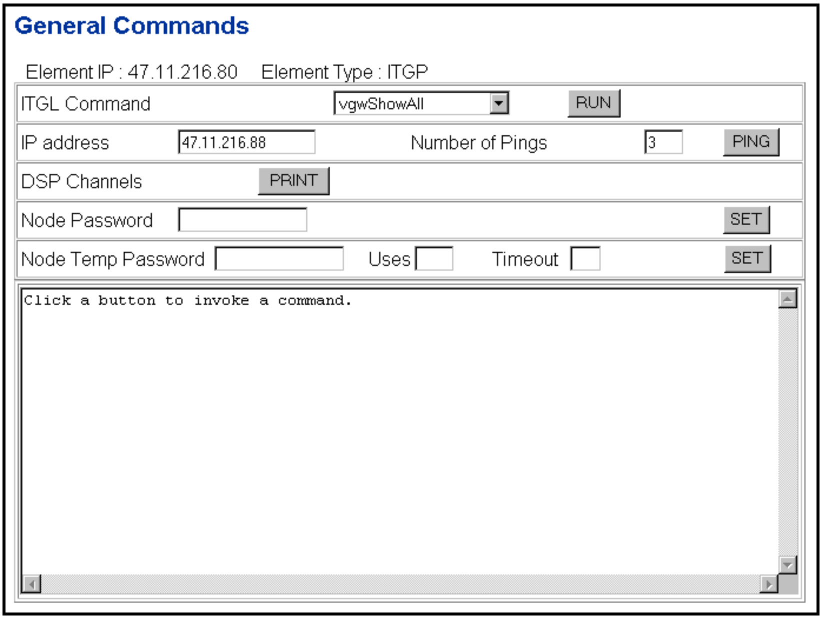
Figure 152
IP Telephony Information



3 Click the **GEN CMD** button associated with the Voice Gateway Media Card.

The **General Commands** pages opens (see Figure 153 on page 546).

Figure 153
General Command



There are three sections of the General commands page that are used to set the Internet Telephone Installer Password. These are the ITGL Command section, the Node Password section, and the Node Temp Password section.

4 In the ITGL Command section, select **nodePwdShow** from the drop-down list box and click **RUN**.

The output of the nodePwdShow command is displayed in the text area at the bottom of the page. If in the default state, the Internet Telephone Installer Password has never been set. The nodePwdShow command should display the following:

```
NodeID   PwdEna    Pwd        TmpPwd     Uses      Timeout
======   =======   ========   ========   =======   ===========
123      No                                        0d 0h 0m 0s
```

where:

NodeID–the Internet Telephone Installer Password configuration applies to all Voice Gateway Media Cards on the same TLAN that belong to this Node ID.

PwdEna–by default the cards should be in disabled state (PwdEna=No). The PwdEna setting specifies the enabled (Yes) or disabled (No) state of the Internet Telephone Installer Password.

Pwd–this is the administrator Internet Telephone Installer Password. In the default state, the administrator password is null.

TmpPwd–this is the temporary Internet Telephone Installer Password. In the default state, the temporary password is null.

Uses–the Uses parameter applies to the temporary Internet Telephone Installer Password. In the default state, this setting is null. If the card is not in the default state, the Uses parameter is a numeric value from 0-1000. This number specifies the remaining number of uses for the temporary password. If zero is entered for the Uses parameter when setting the temporary password, the Time parameter is mandatory. As a result, the password expires based on time instead of a number of uses.

Timeout–the Timeout heading corresponds to the Time parameter of the temporary Internet Telephone Installer Password. In the default state the Time is null. If the card is not in the default state, this setting specifies the duration in hours in which the temporary password is valid. The range is 0-240 hours (which is a maximum of 10 days). The number specified under Timeout indicates the remaining time to expire of the temporary password. The Time parameter is optional if the Uses parameter is non-zero and it is mandatory if Uses is set to zero.

If both the Uses and Time parameters are entered, the password expires on whichever comes first, that is, the Uses parameter is reduced to zero or the Time has expired. If both the Uses and Time parameters are entered and are set to zero, it is the same as not setting the temporary password.

5 Next, set the administrator Internet Telephone Installer Password in the **Node Password** section (see Figure 154 on page 548).

Figure 154
Node Password

This enables and sets the administrator password. The "password" parameter can be null, or 6 to 14 digits. The valid characters are 0-9 * #. This command can be entered at any time. The new password entered overwrites the previous password.

6 Enter a password and click **SET**.

The text area returns the message '**Please run nodePwdShow to verify the result.**"

7 In the ITGL Command section, select **nodePwdShow** from the drop-down list box and click **RUN**.

8 The text area outputs data similar to the following:

NodeID	PwdEna	Pwd	TmpPwd	Uses	Timeout
======	=======	========	========	=======	===========
123	Yes	1234567			0d 0h 0m 0s

WARNING

If the SET button in the Node Password section is clicked and no password is entered in the text box, then the password is enable but is null. In the above output, the PwdEna field displays "Yes" and the Pwd field is blank.

9 To set the Node Temp Password (see Figure 155 on page 549):

- Enter a password in the text box (for example,9876543).
- Enter the number of uses (for example,2).
  The number of uses should be 1 and 1000.
- Enter the timeout value (for example,2).
  The timeout value should be 1 to 240 hours.

Figure 155
Node Temp Password

10 Click **SET**.

The text area returns the message '**Please run nodePwdShow to verify the result.**”

11 In the ITGL Command section, select **nodePwdShow** from the drop-down list box and click **RUN**.

The text area outputs data similar to the following:

NodeID	PwdEna	Pwd	TmpPwd	Uses	Timeout
======	=======	========	========	=======	===========
123	Yes	1234567	9876543	2	0d 2h 0m 0s

12 To clear the temporary Internet Telephone Installer password, select the **nodeTempPwdClear** command from the ITGL Command drop down listbox and then click **RUN**.

13 In the ITGL Command section, select **nodePwdShow** from the drop-down list box and click **RUN**.

The text area outputs data similar to the following:

NodeID	PwdEna	Pwd	TmpPwd	Uses	Timeout
======	=======	========	========	=======	===========
123	Yes	1234567			0d 0h 0m 0s

End of Procedure

Voice Gateway Media Card Maintenance

Contents

This section contains information on the following topics:

Reference list

The following are references for this section:

- *Software Input/Output: System Messages* (553-3001-411)

Overview

This chapter provides information on maintenance functions of the Meridian 1 and Succession Communication Server for Enterprise 1000 Voice Gateway Media Card.

> ***Note:*** Check the Nortel Networks Web site for information on the latest loadware, firmware, and application releases.

Faceplate maintenance display codes

The Voice Gateway Media Card's maintenance display provides the diagnostic status of the card during power-up, its operational state when in service, and error information on the functional state of the card.

- Table 69 on page 553 lists the normal and fault display codes for the ITG-P Line Card.
- Table 70 on page 555 list the normal and fault display codes for the Succession Media Card.

During power-up, the card performs multiple self-tests, including an internal RAM test, ALU test, address mode test, boot ROM test, timer test, and external RAM test. If any of these tests fail, the card enters a maintenance loop, and no further processing is possible. A failure message is printed on the display to indicate which test failed. For example, if the timer test fails on the ITG-P Line Card, F:05 is displayed.

If the other tests fail (up to and including the EEPROM test), a message is displayed for three seconds. If more than one test fails, the message displayed indicates the first failure. If verbose mode has been selected (by the test input pin on the backplane), the three second failure message is not displayed.

If the maintenance display on the ITG-P Line card shows a persistent T:20 indicating an IP Line loadware failure, and if this occurs after the card was reset during a loadware download procedure, call your Nortel Networks technical support for assistance in attempting to download new loadware onto the card.

Table 69
ITG-P Line Card faceplate maintenance display codes (Part 1 of 2)

Normal code	Fault code	Message
T:00	F:00	Initialization
T:01	F:01	Testing Internal RAM
T:02	F:02	Testing ALU
T:03	F:03	Testing address modes
T:04	F:04	Testing Boot ROM
T:05	F:05	Testing timers
T:06	F:06	Testing watchdog
T:07	F:07	Testing external RAM
T:08	F:08	Testing Host DPRAM
T:09	F:09	Testing DS30 DPRAM
T:10	F:10	Testing Security Device
T:11	F:11	Testing Flash memory
T:12	F:12	Programming PCI FPGA
T:13	F:13	Programming DS30 FPGA
T:14	F:14	Programming CEMUX FPGA
T:15	F:15	Programming DSP FPGA
T:16	F:16	Testing CEMUX interface
T:17	F:17	Testing EEPROM

Table 69
ITG-P Line Card faceplate maintenance display codes (Part 2 of 2)

T:18	F:18	Booting processor, waiting for response with self-test information.
T:19	F:19	Waiting for application start-up messages from processor.
T:20		CardLAN enabled, transmitting BootP requests. If this display persists, then the ITG-P Line Card is running in BIOS ROM mode due to card software failure.
T:21		CardLAN operational, A07 enabled, display now under host control. Card is looking for an active Leader by sending BootP requests on the management LAN. If no BootP response is received on the management LAN, Leader 0 times out first and starts active Leader tasks. A Follower card sends BootP requests on the management LAN continuously and never times out. Enter “+++” to escape from BootP request mode and start IPL> shell.
T:22		The ITG-P Line Card is attempting to start the application.
Lxxx		Card is running active Leader tasks where xxx = number of Internet Telephones registered on the card
Fxxx		Card has detected the active Leader and is running Follower tasks, where xxx = number of Internet Telephones registered on the card.

If a test fails on the Succession Media Card, F:XX appears on the Hex display for three seconds after T:13 message (Testing SEEPROM). For example, if the 8051 co-processor test failed, F:05 is displayed on the Succession Media Card faceplate. If more that one test fails, the message indicates the first failure.

Table 70
Succession Media Card faceplate maintenance display codes (Part 1 of 2)

Normal code	Fault code	Message
T:00	F:00	Initialization
T:01	F:01	Testing Internal RAM
T:02	F:02	Testing ALU
T:03	F:03	Testing address modes
T:04	F:04	Testing watchdog
T:05	F:05	Testing 8051 co-processor
T:06	F:06	Testing timers
T:07	F:07	Testing external RAM
T:08	F:08	Testing dongle
T:09	F:09	Programming timeswitch FPGA
T:10	F:10	Programming ISPDI FPGA
T:11	F:11	Testing host dual port RAM
T:12	F:12	Testing DS-30 dual port RAM
T:13	F:13	Testing SEEPROM
T:14	F:14	Booting Host processor, waiting for response with selftest information
T:15	F:15	Not used at present
T:16	F:16	Not used at present

Table 70
Succession Media Card faceplate maintenance display codes (Part 2 of 2)

T:17	F:17	Not used at present
T:18	F:18	Not used at present
T:19	F:19	Not used at present
T:20	F:20	Waiting for application start-up message from Host processor
T:21	F:21	CardLAN enabled, waiting for request configuration message
T:22	F:22	CardLAN operational, A07 enabled, display now under host control

If the IXP encounters any failures during its initialization, an H:XX error code is displayed. Table 71 on page 556 shows the list of error codes.

Table 71
List of error codes for the Succession Media Card

Code	Description
H:00	Host Processor not booting
H:01	SDRAM test failure
H:02	SRAM test failure
H:04	PCMCIA device failure
H:08	Network interface failure
H:10	Meridian 1 interface failure
H:20	DSP interface failure
H:40	NVRAM/EEPROM interface failure
H:80	PCM connector failure

System error messages

When an error or specific event occurs, SNMP sends an alarm trap to OTM or any SNMP manager that is configured in the SNMP Manager's list in the ITG Card properties. It also puts the system error message into the error log file containing error messages.

You can view the error log in OTM IP Line 3.0 application by clicking the **Open Log File** button on the **Maintenance** tab of the **ITG Card Properties**. You can also view the log file in any text browser after uploading it to an FTP host using the LogFilePut command.

ITG and ITS messages incorporate the severity category of the message in the first digit of the four digit number. Message numbers beginning with 0 do not follow this format.

1 = Critical
2 = Major
3 = Minor
4 = Warning
5 = Cleared (Info)
6 = Indeterminate (Info)

Error messages with a severity category of "Critical" are displayed on the Voice Gateway Media Card's maintenance faceplate display in the form: "**Gxxx**" or "**Sxxx**", where **xxx** is the last three digits of the ITG or ITS message. The Signaling Server does not have a faceplate display. Alarms appear in the Signaling Server's report log or by way of SNMP on an Alarm browser.

Table 72 on page 558 lists the critical ITG messages and Table 73 on page 562 lists the critical ITS messages.

All listed alarms can be sent by a Voice Gateway Media Card. Any alarm that can be sent by the Signalling Server has an “X” in the column labeled "Signaling Server."

For a complete listing of other error messages, see *Software Input/Output: System Messages* (553-3001-411).

Table 72
Critical ITG Error messages (Part 1 of 4)

Maintenance Display	Corresponding Critical Error Message	Signaling Server	Description
G000	ITG1000	X	Card (re)booted.
G001	ITG1001	X	Task spawn failure <name>.
G002	ITG1002	X	Memory allocation failure.
G003	ITG1003	X	File IO error <operation> <object> <errno> <errtext>.
G004	ITG1004	X	Network IO error <operation> <object> <errno> <errtext>.
G005	ITG1005	X	Message queue error <operation> <object> <errno> <errtext>.
G006	ITG1006	X	Unexpected state encountered <file> <line> <state>.
G007	ITG1007	X	Unexpected message type <file> <line> <msg>.
G008	ITG1008	X	Null pointer encountered <file> <line> Name of pointer.
G009	ITG1009	X	Invalid block <file> <line> Type of block.

Table 72
Critical ITG Error messages (Part 2 of 4)

Maintenance Display	Corresponding Critical Error Message	Signaling Server	Description
G010	ITG1010	X	Unable to locate data block <file> <line> Type of block.
G011	ITG1011	X	File transfer error: <operation> <file> <host>
G012	ITG1012	X	Module initialization failure: <moduleName>
G013	ITG1013		Ethernet receiver buffer unavailable, packet(s) discarded.
G014	ITG1014	X	Ethernet carrier: <ifName> <state>
G015	ITG1015		Ethernet device failure: <ifName>
G017	ITG1017	X	Invalid or unknown SSD message: <ssdType> <TN> <msg>
G019	ITG1019		DSP channel open failure <channel>.
G020	ITG1020	X	Configuration error <param> <value> <reason>.
G021	ITG1021		DSP successfully reset <dsp>.
G022	ITG1022		DSP channel not responding, channel disabled <channel>.
G023	ITG1023		DSP device failure: <dsp> <errnum> <errtext>
G025	ITG1025		DSP download: <dsp> <reason>
G027	ITG1027		DSP memory test: <dsp> <reason>
G028	ITG1028	X	Voice packet loss: <channel> <%packetLoss> <direction> <dstAddr>

Table 72
Critical ITG Error messages (Part 3 of 4)

Maintenance Display	Corresponding Critical Error Message	Signaling Server	Description
G029	ITG1029		Error in DSP task <file> <line> <errno> <errtext>.
G030	ITG1030		Allocation failure in DSP memory pool.
G031	ITG1031	X	Invalid codec number: <codec>
G032	ITG1032		Attempt to open a DSP that is already open: <channel>
G033	ITG1033		Failed to send data to DSP channel: <channel>
G034	ITG1034		DSP channel unexpectedly closed: <channel>
G035	ITG1035		Encountered and unexpected open DSP channel, closed it: <channel>
G037	ITG1037		Wrong image downloaded. Binary was created for <cardType> card.
G038	ITG1038		IPLlogin protection (login available/locked)
G039	ITG1039		Bad DSP channel <channel id>
G040	ITG1040		Last reset reason for card: <reasonString> where the reason String can be: Reboot command issued (by software or through CLI); Watchdog Timer Expired; Manual reset; Internal XA problem; or Unknown

Table 72
Critical ITG Error messages (Part 4 of 4)

Maintenance Display	Corresponding Critical Error Message	Signaling Server	Description
G041	ITG1041	X	perceivedSeverity = alarmSeverityWarning probableCause = alarmCauseRemoteTransmissionError OTM displays the text “F/W file(s) not received but internet phones have registered. May have mixed F/W versions across phones. When F/W file(s) received, internet phones will automatically be updated.”
G042	ITG1042		perceivedSeverity = alarmSeverityWarning probableCause = alarmCauseOutOfMemory OTM displays the text “Insufficient flash drive space to store F/W file.”

Table 73
Critical ITS Error messages (Part 1 of 2)

Maintenance Display	Corresponding Critical Error Message	Signaling Server	Description
S000	ITS1000	X	VTI function call timeout.
S001	ITS1001	X	User terminal registration failed. <ip> <hwid> <errno> <errtext>.
S002	ITS1002	X	Connect service activation error <reason>.
S003	ITS1003	X	Duplicate master <node> <ip1> <ip2>.
S004	ITS1004	X	Invalid node ID <ip> <hwid>.
S005	ITS1005	X	Corrupted node ID/TN field <ip> <hwid>.
S006	ITS1006	X	Received corrupted UNIStim message <message dump>.
S007	ITS1007	X	Received unknown UNIStim message <message dump>.
S008	ITS1008	X	Terminal connection status: <ip> <status>.
S009	ITS1009	X	Call Server communication link:<state>.
S010	ITS1010	X	Terminal doesn't support Codec: <ip><codec>.
S011	ITS1011	X	<IP Address>: Last reset reason for phone: <reasonID> (<reasonString>)

Table 73
Critical ITS Error messages (Part 2 of 2)

Maintenance Display	Corresponding Critical Error Message	Signaling Server	Description
S012	ITS1012	X	User entered the wrong Internet Telephone Installer Password three times during Branch User Config.The set is locked out from doing any User Config for one hour. Action: Wait for the set to unlock in one hour, or use the IPL CLI command clearLockout to unlock the set.
S013	ITS1013	X	User entered the wrong Craftsperson Node Level TN Entry Password three times.The set is locked out. Action: To remove the lock, use Overlay 32 to disable, and then enable the Internet Telephone.

IP Line and Internet Telephone maintenance and diagnostics - LD 32

For Nortel Networks Internet Telephones, there are two kinds of TNs to consider:

- Physical TN, that represents a physical unit of the Voice Gateway Media Card
- Virtual TN, that is configured on a virtual superloop and represents an Internet Telephone

Physical TNs, that are seen as trunk units, are managed using existing LD 32 commands.

Because virtual TNs are configured on a virtual superloop, Virtual TN maintenance has no meaning, that is, what is already provided by the Meridian 1 and Succession CSE 1000 for phantom loops. In LD 32, any command affecting a phantom loop leads to an NTP665 message because the loop does not physically exist. LD 32 supports STAT, DISU, ENLU, and IDU commands on an Internet Telephone Virtual TN. All other commands lead to the new NPR047 message.

The IDU command provides information such as

- TN
- TNID
- NT code
- color code
- release code
- serial number
- IP address of the
- IP address of the Voice Gateway Media Card that is acting as the terminal proxy

The serial number is the last three bytes of the Internet Telephone's MAC address, printed in ASCII hexadecimal format.

Since the Meridian 1 and Succession CSE 1000 must request the information from the Internet Telephone, the IDU is effectively a PING command and can be used to test the end-to-end IP connectivity of the Internet Telephone. The output format of the IDU command in LD 32 is shown in Table 74. This format applies only for Internet Telephone Virtual TNs. Table 75 on page 566 contains the maintenance commands in LD 32 for the Internet Telephone.

If the Internet Telephone is not registered with the Meridian 1 and Succession CSE 1000, an NPR0048 message is generated. If the Internet Telephone is registered but idle, the system prints the Internet Telephone IP address and Voice Gateway Media Card IP address and generates an NPR0053 message.

Table 74
IDU command printout in LD 32

Item	Description
ISET TN:	l s c u
TN ID CODE:	i2002, i2004, or i2050
NT CODE:	xxxxxx
COLOR CODE:	xx
RLS CODE:	xx
SER NUM:	xxxxxxx
SET IP ADR:	xxx.xxx.xxx.xxx
TPS IP ADR:	xxx.xxx.xxx.xxx

Table 75
LD 32 Maintenance Commands for Internet Telephones

Prompt	Response	Description
STAT l s c u STAT cu	UNEQ IDLE REGISTERED IDLE UNREGISTERED BUSY DSBL REGISTERED DSBL UNREGISTERED	Display the Internet Telephone state. UNEQ, IDLE, BUSY, and DSBL have the usual meaning. IDLE and DSBL state are precise by the following information: • UNREGISTERED identifies an Internet Telephone that is configured in the system but that has not yet registered. • REGISTERED identifies an Internet Telephone that has registered.
DISU l s c u DISU cu	OK	Change the Internet Telephone state to DSBL. UNREGISTERED/REGISTERED state is not modified.
ENLU l s c u ENLU cu	OK	Change the Internet Telephone state to IDLE. UNREGISTERED/REGISTERED state is not modified.
IDU l s c u IDU cu	Displays the TN number, device code, NT code, color code, release code, and the last three bytes of the MAC address. Displays the IP address for Internet Telephones and the Terminal Proxy Server.	Displays selected Internet Telephone information.

IP Line CLI commands

IP Line CLI commands are designed to supplement Overlay commands and to introduce new features specific to the ITG-P Line Card, Succession Media Card, and Signaling Server platforms.

All the CLI commands listed in Table 76 to Table 88 are supported on the ITG-P Line Card and Succession Media Card. The CLI commands are also available on the Signaling Server if an “X” is shown in the Signaling Server column of the table.

The IP Line CLI commands are accessed by connecting a TTY to the MAINT port on the Voice Gateway Media Card faceplate. Alternatively, the Telnet command can be used to access the CLI. These IP Line CLI commands are entered at the **IPL>** prompt. Instructions for connecting to the maintenance port of the Signaling Server are described in *Installation and Configuration* (553-3023-210). Refer to the “Signaling Server maintenance ports” section.

The commands are grouped into the following categories:

- “General Purpose commands” on page 568
- “File Transfer commands” on page 571
- “IP Configuration commands” on page 575
- “Reset commands” on page 576
- “DSP commands” on page 576
- “Upgrade commands” on page 577
- “IPL> Shell command” on page 577
- “Internet Telephone Installer Password commands” on page 578
- “VGW commands” on page 580
- “Data Path Capture Tool commands” on page 580
- “Graceful Disable commands” on page 581
- “Patching Tool commands” on page 582
- “Audit commands” on page 582

Table 76 lists the general purpose IPL> commands.

Table 76
General Purpose commands (Part 1 of 3)

IPL> Command	Description	Signaling Server
i	Displays the current task list.	X
itgHelp	Displays the complete command list. **?** also shows the command list.	
logout	Exits the IPL> Command Line Interface.	
routeAdd	Adds a route to the network routing table.	X
routeShow	Displays the current host and network routing tables.	X
logPrintOff	Turns off logging in the TTY session where you are currently logged in.	
logPrintOn	Turns on logging in the TTY session where you are currently logged in.	
chkdsk	chkdsk "/C:" Checks the internal file system for errors. chkdsk "/C:", 1 Repairs the file system errors and saves the damaged cluster in files. chkdsk "/C:", 2 Repairs file system errors and returns damaged clusters to the free pool.	

Table 76
General Purpose commands (Part 2 of 3)

IPL> Command	Description	Signaling Server
ping "host", "numpackets"	Sends an ICMP ECHO_REQUEST packet to a network host. The host matching the destination address in the packets responds to the request. If a response is not returned, the sender times out. This command is useful to determine if other hosts or Voice Gateway Media Cards are communicating with the sender card. The "numpackets" parameter specifies how many packets to send. If it is not included, ping runs until it is stopped by Ctrl-C (that also exits the IPL> Command Line Interface). Example: IPL> **ping** "47.82.33.123", 10	X
itgCardShow	Displays Voice Gateway Media Card information.	X
itgMemShow	Displays memory usage.	X
ifShow	Displays detailed IP information, including MAC addresses.	X
IPInfoShow	Displays IP information.	X
serialNumShow	Displays card serial number. This command displays the same Voice Gateway Media Card serial number that is displayed in the LD 32 IDC command.	
firmwareVersionShow	Displays firmware version number.	
numChannelsShow	Displays number of available channels.	
swVersionShow	Displays software version.	X
logFileOn	Turns on error logging to the syslog file.	
logFileOff	Turns off error logging to the syslog file.	

Table 76
General Purpose commands (Part 3 of 3)

IPL> Command	Description	Signaling Server
logShow	Displays information about the current logging configuration. Indicates whether logging is on or off.	
logConsoleOn	Turns on error logging to the console.	
logConsoleOff	Turns off error logging to the console.	
isetShow	Displays general information for all registered Internet Telephones. For example, the command displays the IP address of the Internet Telephone, the VTN that the Internet Telephone is associated with, indicates the type of Internet Telephone such as i2002, i2004, or i2050, and provides the type of registration and the new registration status.	X
isetShowByTN	Displays general information about all registered Internet Telephones, sorted by TN.	X
isetShowByIP	Displays general information about all registered Internet Telephones, sorted by IP address.	X
pbxLinkShow	Displays information about the link to the CPU, including the configuration and link status.	X
itgAlarmTest	Generates **ITGxxxx** test alarms.	X
itsAlarmTest	Generates **ITSxxxx** test alarms.	X
itgPLThreshold	Sets the Internet Telephone and gateway alarm packet loss threshold (units 0.1%). An alarm is generated when the threshold is reached.	
elmShow	Displays a list of supported languages.	X
itgChanStateShow	Displays the state for channels, for example, if they are idle or busy.	

Table 77 lists the file transfer commands.

Table 77
File Transfer commands (Part 1 of 4)

IPL> Commands	Description	Signaling Server
swDownload "hostname", "username", "password", "directory path", "filename"	Loads a new version of software from the FTP host to the Voice Gateway Media Card. Updates the software on the Voice Gateway Media Card with the binary file received from an FTP server corresponding to the *hostname* IP address. The Voice Gateway Media Card FTP client performs a Get which downloads the file to the flash bank. A checksum is calculated to verify correct delivery. Once the new software version is successfully downloaded, the Voice Gateway Media Card must be rebooted with cardReset to run the new software. ***Note:*** *Hostname* refers to the either IP address of the FTP host, or the Voice Gateway Media Card itself or another Voice Gateway Media Card when a PC card in the /A: drive of the Voice Gateway Media Card contains the software binary file. Example: IPL> **swDownload** "47.82.32.346", "anonymous", "guest", "/software", "VxWorks.mms"	

Table 77
File Transfer commands (Part 2 of 4)

IPL> Commands	Description	Signaling Server
configFileGet "hostname", "username", "password", "directory path", "filename"	Sends an updated CONFIG.INI file from OTM to the Voice Gateway Media Card. Updates the CONFIG.INI file on the Voice Gateway Media Card with the CONFIG.INI file on the specified host, account, and path. The configFileGet task on the ITG host initiates an FTP session with the given parameters and downloads the file to flash file system. The CONFIG.INI file also contains the gatekeeper IP address, gateway password, and gateway DN-port mapping table. Example: IPL> **configFileGet** "ngals042", "anonymous", "guest", "/configDir", "config.ini"	X
bootPFileGet "hostname", "username", "password", "directory path", "filename"	Updates the BOOTPtab file on the Voice Gateway Media Card with the BOOTPtab file on the specified host, account and path. The bootpFileGet task on the ITG host initiates an FTP session with the given parameters and downloads the file to flash file system. Example: IPL> **bootPFileGet** "ngals042", "anonymous", "guest", "/bootpDir", "bootptab"	X

Table 77
File Transfer commands (Part 3 of 4)

IPL> Commands	Description	Signaling Server
hostFileGet "hostname", "username", "password", "directory path", "filename", "ITGFileName", listener	Transfers any file from OTM to the Voice Gateway Media Card. This command gets any file from the host and does a Get using FTP to the Voice Gateway Media Card. ***Note:*** ITGFileName is the full path AND filename of where the file is to be placed. The listener parameter indicates which module to inform of the successful file transfer. It can be set to –1 to be disabled. Example: IPL> **hostFileGet** "ngals042", "anonymous", "guest", "/hostfileDir", "hostFile.txt", "/C:ITGFILRDIR/ITGFILE.TXT", -1	X
currOMFilePut "hostname", "username", "password", "directory path", "filename"	Sends the current Operational Measurements (OM) file to the specified host. The OMFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the Voice Gateway Media Card's Operational Measurements file to the specified location on the host. Example: IPL> **currOMFilePut** "ngals042", "anonymous", "guest", "/currDir", "omFile"	X
prevOMFilePut "hostname", "username", "password", "directory path", "filename"	Sends the previous Operational Measurements (OM) file to the specified host. The OMFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the Voice Gateway Media Card's Operational Measurements file to the specified location on the host. Example: IPL> **prevOMFilePut** "ngals042", "anonymous", "guest", "/prevDir", "omFile"	

Table 77
File Transfer commands (Part 4 of 4)

IPL> Commands	Description	Signaling Server
LogFilePut "hostname", "username", "password", "directory path", "filename"	Sends the syslog file from the Voice Gateway Media Card to OTM. The LogFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the Voice Gateway Media Card's logfile to the specified location on the host. Example: IPL> **LogFilePut** "ngals042", "anonymous", "guest", "/currDir", "logFile"	
bootPFilePut "hostname", "username", "password", "directory path", "filename"	Sends the BOOTPtab file from the Voice Gateway Media Card to OTM. Example: IPL> **bootPFilePut** "ngals042", "anonymous", "guest", "/bootpDir", "bootpFile"	X
hostFilePut "hostname", "username", "password", "directory path", "filename", ITGFileName	Transfers any file from the Voice Gateway Media Card to the OTM PC. Example: IPL> **hostFilePut** "ngals042", "anonymous", "guest", "/hostDir", "hostFile", "/C:/CONFIG/CONFIG1.INI"	X
omFilePut "hostname", "username", "password", "directory path", "filename", ITGFileName	Sends the current Operational Measurements (OM) file to the specified host. Example: IPL> **OMFilePut** "ngals042", "anonymous", "guest", "/hostDir", "omFile"	X

Table 78 lists the IP configuration IPL> commands.

Table 78
IP Configuration commands

IPL> Command	Description	Signaling Server
NVRIPSet	Sets the IP address in NVRAM.	
NVRGWSet	Sets the default gateway address in NVRAM.	
NVRSMSet	Sets the subnet mask in NVRAM.	
NVRIPShow	Prints the values of the IP parameters that reside in NVRAM.	
NVRClear	Clear IP parameters in NVRAM.	
nvramLeaderSet	Sets the Leader bit in NVRAM.	
nvramLeaderClr	Clears the Leader bit in NVRAM, but does not erase the IP parameters in NVRAM.	
setLeader	Sets a Leader card, including the IP address, gateway, subnet mask, boot method to static, and Leader bit in NVRAM. This one command does all the necessary actions to make a Leader.	
clearLeader	Clears the Leader information in NVRAM, sets the boot method to use BOOTP, and removes the old configuration files. This command makes a Leader card into a Follower card.	
tLanDuplexSet	Sets the TLAN Ethernet duplex mode.	
tLanSpeedSet	Sets the TLAN Ethernet speed.	

Table 79 lists the reset IPL> commands.

Table 79
Reset commands

IPL> Command	Description	Signaling Server
cardReset	Resets a Voice Gateway Media Card. This command performs a warm reboot of the Voice Gateway Media Card. The card must be in the OOS state to use this command.	
isetReset "tn" l s c u **isetReset "tn" c u**	Resets the Internet Telephone on Option 51C/61C/81/81C. Resets the Internet Telephone on Option 11C/11C-Mini and Succession CSE 1000 systems.	X
isetResetAll	Resets all registered Internet Telephones.	X
resetOM	Resets the operational measurement file timer. This command resets all operational measurement parameters collected since last log dump.	X
lastResetReason	Displays the reason for the last card reset.	

Table 80 lists the DSP IPL> commands applicable to the Voice Gateway Media Card.

Table 80
DSP commands

IPL> Command	Description	Signaling Server
DSPReset	Resets the specified DSP.	
DSPNumShow	Displays the number of DSPs on the Voice Gateway Media Card.	

Table 81 lists the upgrade IPL> commands.

Table 81
Upgrade commands

IPL> Command	Description	Signaling Server
umsPolicyShow	Displays the current upgrade policy.	X
umsUpgradeAll	Upgrades all registered telephones according to policy and firmware file.	X
umsUpgradeTimerShow	Shows the upgrade schedule.	X
umsUpgradeTimerCancel	Cancels the scheduled upgrade.	X

Table 82 lists the command to change the IPL> shell password.

Table 82
IPL> Shell command

IPL> command	Description	Signaling Server
shellPasswordSet	Changes the current user name and password of the IPL> CLI shell.	

Table 83 lists the Internet Telephone Installer Password commands.

Table 83
Internet Telephone Installer Password commands (Part 1 of 2)

IPL> command	Description	Signaling Server
nodePwdSet "password"	Sets and enables the administrative Internet Telephone Installer (node) Password. This is also known as the node level Internet Telephone Installer Password. If a null password (0-length) is configured, all Internet Telephones that attempt to register after this command has been issued display a prompt for node password before the TN can be modified. The "password" parameter must be null or 6 to 14 digits in length; The valid characters are 0-9 * #. The null password causes the Node ID and Password screen on the Internet Telephone to be skipped during restart. This command can be entered at any time; the new password entered overwrites the prior password.	X
nodePwdShow	Displays the settings of the Internet Telephone Installer Password. The command displays the current password, the state of password entry (enable/disable), the temporary password, and the number of uses and time to expiry.	X
nodePwdEnable	Enables the administrative Internet Telephone Installer Password setting. After this command is entered, all Internet Telephones registering display the password screen.	X
nodePwdDisable	Disables both the administrative and the temporary Internet Telephone Installer Password settings. After this command is entered, all Internet Telephones display the original Node ID and TN screen during registration.	X

Table 83
Internet Telephone Installer Password commands (Part 2 of 2)

IPL> command	Description	Signaling Server
nodeTempPwdSet "tempPwd", uses, <time>	Sets the temporary Internet Telephone Installer Password. This password is disabled by default. The password must be a string 6 to 14 digits in length. A null password cannot be entered. The valid tempPwd characters are 0-9 * #. The uses parameter is a numeric value from 0-1000. This parameter specifies the number of uses for which the temporary password is valid. The range for the time parameter is 0-240 hours, which is a maximum of 10 days. The time parameter specifies the duration in hours that the password is valid. • If the uses parameter is set to zero, the time parameter is mandatory. As a result, the password only expires based on time. • If the uses parameter is non-zero, the time parameter is optional. • If both the uses and time parameters are entered, the password expires on whichever comes first, that is, uses is reduced to zero or the time has expired. • If both uses and time are entered and both are set to zero, it is the same as not setting the temporary password at all. This command can be entered at any time and the new parameters overwrite the existing temporary password's parameters.	X
nodeTempPwdClear	Deletes the temporary Internet Telephone Installer Password. It also reset the uses and time parameters to zero.	X

Table 84 lists the Voice Gateway commands used on the Voice Gateway Media Card.

Table 84
VGW commands

IPL> command	Description	Signaling Server
vgwPLLog	Toggles gateway packet loss logging on and off.	
vgwShow	Displays information about the active (non-idle and equipped) gateway channels. Entering this command with the IP address of an Internet Telephone at the Command Line Interface of any node's Voice Gateway Media Card displays the identification of the card that has a gateway channel in use by the Internet Telephone. This is useful when you need to identify from which card to collect gateway statistics (for example, packet loss).	
vgwShowALL	Displays information about all gateway channels.	

Table 85 lists the commands used with the Data Path Capture Tool.

Table 85
Data Path Capture Tool commands (Part 1 of 2)

IPL> command	Description	Signaling Server
captureStart	Begins the capture operation. When the command is entered, data for the gateway channel <tcid> (0-23 for ITG-P Line Card and 0-31 for Succession Media Card) begins to be captured to the circular queue.	
captureStop	Stops the audio data capture.	
captureSaveLocal	Dumps the contents of the circular queue to the specified file on the memory PC card inserted in the /A: drive on the Voice Gateway Media Card's faceplate.	

Table 85
Data Path Capture Tool commands (Part 2 of 2)

IPL> command	Description	Signaling Server
captureSaveRemote	FTPs the contents of the circular queue to the specified file on the remote server.	
captureFree	Frees the capture queue.	

Table 86 lists the commands used to gracefully disable the TPS and Voice gateway services and the commands to enable these services after they have been disabled.

Table 86
Graceful Disable commands

IPL> command	Description	Signaling Server
disiAll	Gracefully disables both the LTPS and voice gateway service on the Voice Gateway Media Card. Gracefully disables the LTPS on the Signaling Server.	X
disiTPS	Gracefully disables the LTPS service on the Voice Gateway Media Card. Prevents new Internet Telephones registering on the card, and all registered Internet Telephones are redirected to another card when idle.	X
disiVGW	Gracefully disables voice gateway service.	
enaAll	Enables both the LTPS and voice gateway service on the Voice Gateway Media Card. Enables the LTPS on the Signaling Server.	X
enaTPS	Enables the LTPS service.	X
enaVGW	Enables the voice gateway service.	

Table 87 lists the Patching Tool commands.

Table 87
Patching Tool commands

IPL> command	Description	Signaling Server
pins	Puts a patch into service that has been loaded into memory using the pload command.	X
plis	Gives detailed patch status information for a loaded patch.	X
pload	Loads a patch file from the file system on Flash memory into DRAM memory	X
pnew	Creates memory patches for the Voice Gateway Media Card.	X
poos	Deactivates a patch by restoring the patched procedure to its original state.	X
pout	Removes a patch from DRAM memory.	X
pstat	Gives summary status for one or all loaded patches.	X

Table 88 lists the Audit commands.

Table 88
Audit commands (Part 1 of 2)

Command	Description	Signaling Server
auditHistoryShow	Displays the recent history of the audit task's activity.	
auditRebootSet	Distributes globally the audit task from resetting the card.	
auditRebootTimeSet	Sets the time of non-critical task triggered card resets.	

Table 88
Audit commands (Part 2 of 2)

Command	Description	Signaling Server
auditShow	Displays audit task information, such as a list of tasks and the time for non-critical tasks triggered resets.	
auditTaskSet	Enables manual setting of a task to critical or non-critical status.	

Voice Gateway Media Card self-tests

During power-up, the Voice Gateway Media Card performs diagnostic tests to ensure correct operation. The faceplate RS-232 port on the Voice Gateway Media Card can be used to monitor the progress of these tests. When the processor responds correctly, the 8051XA controller switchs its serial port to provide Card LAN communication and connects the processor with the external RS-232 port.

Troubleshooting a loadware load failure

Symptoms

OTM cannot establish connection with Voice Gateway Media Card. The faceplate LCD display reads "BIOS."

Problem

The Voice Gateway Media Card has booted the BIOS load.

Diagnosis

In the event of a failure to load and run the IP Line loadware, the Voice Gateway Media Card defaults to the BIOS load. This load consists of a prompt that enables commands to reload the IP Line loadware and reboot (see below).

There are three known reasons for the failure to load the IP Line loadware:

- Not enough memory due to a faulty or missing SIMM.

- Corruption of the IP Line loadware image in flash memory.
- The escape sequence to boot from the BIOS has been inadvertently sent down the serial line due to noise.

To determine the cause of the IP Line load failure, reboot and monitor the booting sequence through the serial port. Capture the booting sequence to aid in communication with technical support personnel.

Examples of booting sequences

Case 1

The following excerpt from the booting sequence indicates the amount of memory onboard.

Memory Configuration
Onboard: 4MB
SIMM: 16MB
Total: 20MB

In the absence or failure of the SIMM, the total memory is 4MB, that is not enough to support the IP Line application.

Case 2

The following excerpt from the booting sequence indicates the Voice Gateway Media Card locating and loading the IP Line loadware from flash memory:

Cookie array value: 0x111111100

Checksum Validation at Bank Address: 0xF9800000
Checksum in ROM = 35582602
Length of bank = 0004FEF8
Calculated Checksum = 35582602

Checksum array value: 0x11111100

Loading code from address: F9800010
Verifying ROM to RAM copy...
ROM to RAM copy completed OK
Jumping to VxWorks at 0x00E00000
EIP = 0x00E0011E
Jumping to romStart at 0x00E00300

In the event of a loadware load failure, the boot sequence indicates that the BIOS is being loaded:

Cookie array value: 0x11111111
Booting from BIOS ROM

Case 3

The boot sequence indicates that the "xxx" sequence has been entered and the BIOS is being loaded.

Solutions

Case 1

If a SIMM is missing, install a 16MB SIMM into the SIMM slot which is underneath the daughterboard. If the SIMM is present, check that the SIMM is properly seated. Otherwise, the SIMM is faulty and needs replacement.

Case 2

Re-attempt a loadware download from the OTM host. Use the following commands:

upgradeErase
upgrade "hostname","hostAccount","hostPassword", "hostDirectoryPath","hostSWFilename"

After the loadware loads to flash, reboot the card:

sysReboot

If the failure to load the IP Line loadware into RAM persists, then the flash device is faulty. Replace the Voice Gateway Media Card.

Case 3

The escape sequence "xxx" is rarely transmitted. Reboot the card.

Warm rebooting the Voice Gateway Media Card

The following IP Line CLI command performs a warm reboot of an out-of-service Voice Gateway Media Card: **cardReset**

Testing the Voice Gateway Media Card DSPs

At the IPL> CLI, the following two tests can be performed on the IP Line DSPs:

- To run a self-test on the DSP daughterboard: **DSPselfTest**

  Note: If the DSP self-test fails, the Voice Gateway Media Card must be replaced.

- To run a PCM loopback test, a Send loopback test, or a Receive loopback test on the DSP daughterboard, respectively:

  DSPPcmLpbkTestOn ("DSPPcmLpbkTestOff" to stop the test)
  DSPSndLpbkTestOn ("DSPSndLpbkTestOff" to stop the test)
  DSPRcvLpbkTestOn ("DSPRcvLpbkTestOff" to stop the test)

  Note: The DSPs and all associated ports must be disabled before performing these tests.

Work with alarm and log files

Alarm and log file output is turned on using the IPL> CLI. The following commands can be performed at the IPL> prompt:

- To turn on or turn off the error log file, type: **logFileOn** or **logFileOff**.
- To display the modes of all log files and alarms, type: **logFileShow**.

Troubleshooting Internet Telephone Installation

If you are unable to install an Internet Telephone because the prompt for the node ID or TN does not display:

- Log in to one Voice Gateway Media Card in the node.
- Type the **nodePwdShow** command at the IPL> prompt.
- If the administrative password is enabled (PwdEna=Yes) and there is a null (zero-length) password, that is, the Pwd field is blank, then Internet Telephone cannot be installed Internet Telephone on that Voice Gateway Media Card.

```
NodeID    PwdEna    Pwd        TmpPwd     Uses      Timeout
======    =======   ========   ========   =======   ==========
123       Yes                                       0d 0h 0m 0s
```

- Use the **nodePwdSet "password"** command to set the administrative password and to enable telephones to be installed. Ensure the "password" parameter is included.

Maintenance Telephone

An Internet Telephone functions as a maintenance telephone when you define the class-of-service as MTA (Maintenance Telephone Allowed) in the Multi-line Telephone Administration program (LD 11). A maintenance telephone enables you to send commands to the system, but you can use only a subset of the commands that can be entered from a system terminal. To access the system using the maintenance telephone, a Special Service Prefix (SPRE) code (defined in the customer data block) is entered and followed by "91". To enter commands, press the keys that correspond to the letters and numbers of the command (for example, to enter LD 42 return, key in 53#42##).

The following Overlays (OVLs) are accessible from an Internet Telephone operating as a maintenance telephone: 30, 32, 33, 34, 36, 37, 38, 41, 42, 43, 45, 46, 60, and 62.

Note: The above maintenance overlay operations are supported on Internet Telephones except for the Tone and Digit Switch (TDS) commands of LD 34 and TONE command of LD 46.

Upgrading Voice Gateway Media Card firmware

The minimum versions of the card firmware for the Voice Gateway Media Card are:

- Version 6.4 for the Succession Media Card
- Version 5.6 for the ITG-P Line Card

Check the Nortel Networks Web site for the most current version of the firmware. To download firmware files from Nortel Networks, see Procedure 111 on page 719.

Once the most current version of the firmware has been downloaded, follow the steps in:

- Procedure 90 on page 590 to upgrade the firmware on the ITG-P Line Card
- Procedure 91 on page 592 to upgrade the firmware on the Succession Media Card

Upgrading the ITG-P Line Card firmware

The following procedure upgrades the firmware on the ITG-P Line Cards. Enter all the upgrade commands at the VxWorks shell prompt. Copy the F/W binary file (on a PC Card plugged into the card's faceplate) to the card's /C: drive or to a network server accessible by the card.

Procedure 90
Upgrading the ITG-P Line Card firmware

1 Check if the firmware upgrade is required. Check the firmware version by entering the firmwareVersionShow command:

IPL> firmwareVersionShow
Firmware Version = ITG Firmware Rls 4.0
value = 40 = 0x28 = '('
IPL>

Note: If the F/W version is version 5.6 or greater, the upgrade is not needed.

2 Depending on the location of the firmware file, enter one of the following commands as shown in Table 89:

Table 89
Upgrade command based on file location

— File is located on the card's /C: drive (The file was previously FTPed to /C:): upgradeXa “127.0.0.1","userid","password","</C:/path>","<fw_filename>"
— File is located on a PC Card plugged in the card’s faceplate: upgradeXa "127.0.0.1","userid","password","</A:/path>","<fw_filename>"
— File is located on another card’s /C: drive (The file was previously FTPed to /C:): upgradeXa "<ITG ELAN IPaddr>","userid","password","<path>","<fwfilename>"
— File is located on the OTM PC: upgradeXa "<PC’s IP addr>","itguser","itguser","","<fw_filename>"
— File is located on a network FTP server: upgradeXa "<server’s IP addr>","<uid>","<pswd>","<path>","<fw_filename>"

3 If the upgrade process is successful, the following is displayed:

Upgrade packet: 0..100..200..300..400..500..600..700..800..
tUpgradeXa: 8051XA Upgrade completed OK
tUpgradeXa: Reboot the pack to run new loadware

Note: If these messages do not display, the upgrade was not successful. Repeat step 2 again. Do not continue with steps 4 and 5.

4 Reboot the card if both of the following are true:

- the download is successful
- the firmware version on the card that was checked in step 1 is version 4.0 or later

However, if the firmware version is prior to version 4.0, enter the following commands:

```
xaSend 0,0x11
W 05555,AA
W 02AAA,55
W 05555,80
W 05555,AA
W 02AAA,55
W 05555,30
```

Note 1: There is a space after xaSend and the letter “W”. No other spaces are allowed. All letters are in uppercase.

Note 2: Ignore any syntax error messages that print out after the xaSend command is entered.

After the last command is entered, the card automatically reboots.

5 When the card boots up with firmware version x.x, the following messages are printed:

```
ITG Firmware Rls x.x
8051XA Firmware Version x.x (Pentium) <date>
(C) Nortel Networks Inc., 1996-2001
32K External RAM detected
All FPGAs are configured
No dongle detected
8K DPRAM detected

Bank 0 Checksum - 54A9H
....
```

End of Procedure

Upgrading the Succession Media Card firmware

Upgrades of the Succession Media Card firmware can be required at times. For instance, the firmware can be upgraded to enable the display of the last reset reason. If the SMC is a Release 8 vintage or older, it cannot be upgraded unless the 8051 OTP part is changed on the board. Vintages of the card after Release 8 can be upgraded as described in this section. The release label is on the faceplate (below the Hex display).

Procedure 91
Upgrading the Succession Media Card firmware

1 Check if the firmware upgrade is required and if the card can have its firmware upgraded by this process.

```
IPL> firmwareVersionShow
Firmware Version = ITG Firmware Rls 6.0
value = 40 = 0x28 = '('
IPL>
```

2 Check the release label on the faceplate (below the Hex display) and ensure it is newer than Release 8.

3 Reboot the card.

While the card is booting, break into the BIOS by entering **jkl** when prompted.

4 At the prompt enter the following commands:

```
-> initMm
value = 0 = 0x0
-> spawnMm
value = 0 = 0x0
```

5 Depending on the location of the firmware file, enter one of the following commands as shown in Table 90.

Table 90
Upgrade command based on file location

—	File is located on the card's /C: drive (The file was previously FTPed to /C:): upgradeXa “127.0.0.1","userid","password","</C:/path>","<fw_filename>"
—	File is located on a PC Card plugged in the card’s faceplate: upgradeXa "127.0.0.1","userid","password","</A:/path>","<fw_filename>"
—	File is located on another card’s /C: drive (The file was previously FTPed to /C:): upgradeXa "<ITG ELAN IPaddr>","userid","password","<path>","<fwfilename>"
—	File is located on the OTM PC: upgradeXa "<PC’s IP addr>","itguser","itguser","","<fw_filename>"
—	File is located on a network FTP server: upgradeXa "<server’s IP addr>","<uid>","<pswd>","<path>","<fw_filename>"

6 If the upgrade process is successful, the following is displayed:

Upgrade packet:
0..100..200..300..400..500..600..700..800..900..1000..1100..1200..
1300..1400..1500..1600..1700..1800..1900..
tUpgradeXa: 8051XA Upgrade completed OK
tUpgradeXa: Reboot the pack to run new loadware

Note: If the upgrade is not successful, these messages do not display. Repeat step 5 again.

7 Reboot the card.

8 When the card boots up with version 6.0 firmware (for instance), the following messages are printed:

MC Firmware Rls 6.0
8051XA Firmware Version 4.5 8 February 2002
(C) Nortel Inc. 2001
EPLD Version: 3.0
32K External RAM detected
8K DPRAM detected
All FPGAs are configured
No dongle detected

Bank 1 Checksum - 7354H
SRAM test okay
SDRAM Addr test okay
....

End of Procedure

Replacing the Succession Media Card's CompactFlash

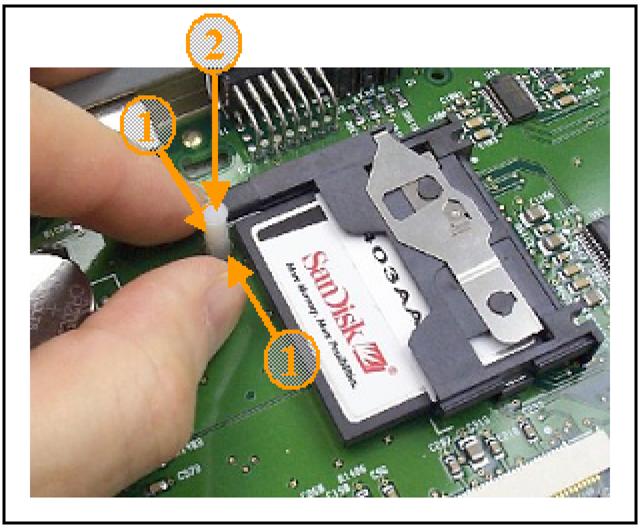
The Succession Media Card must have the CompactFlash card installed in order to be used as a Voice Gateway Media Card. If the CompactFlash card is removed from the Succession Media Card, another CompactFlash card must be installed prior to using the Succession Media Card.

If it is necessary to remove the CompactFlash card, follow the steps in Procedure 92 on page 595. To reinstall a CompactFlash card, see Procedure 6 on page 232.

Procedure 92
Removing the CompactFlash

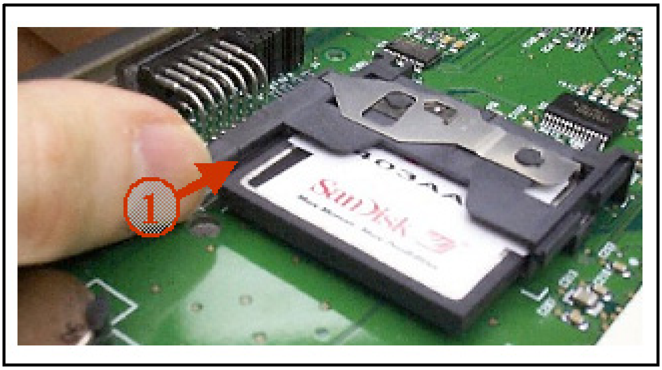
1 Squeeze the tangs at the base of the Retaining Pin (the tangs are labeled **1** in Figure 156). Continue to squeeze the tangs and press the Retaining Pin down to remove it from the card (labeled **2** in Figure 156).

Figure 156
Squeeze the Retaining Pin tangs



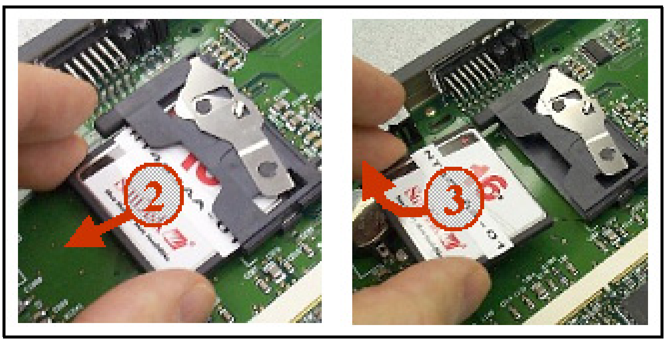
2 Press the Eject button to release the CompactFlash card from the socket (see **1** in Figure 157).

Figure 157
Press Eject button



3 Slide the card out of the socket (labeled **2** in Figure 158) and carefully remove the CompactFlash card (labeled **3** in Figure 158).

Figure 158
Removing the CompactFlash card



4 Return the CompactFlash card to an anti-static package.

End of Procedure

Voice Gateway Media Card Maintenance using OTM 2.0

Contents

This section contains information on the following topics:

Reference list

The following are references for this section:

- *Installing and Configuring Optivity Telephony Manager* (553-3001-230)
- *Using Optivity Telephony Manager* (553-3001-330)
- *Upgrades* (553-3023-258)

Overview

This chapter provides information for using Optivity Telephony Management (OTM) to perform maintenance functions on the Meridian 1 and Succession Communication Server for Enterprise (CSE) 1000 Rel 1.1 Voice Gateway Media Card.

Where reference is made to OTM, the latest version, OTM 2.0, is assumed.

> **CAUTION — Service Interruption**
>
> This procedure in this chapter are not supported for a node which resides on a Succession CSE 1000 Rel 2.0 system.

Replacing a Voice Gateway Media Card

Replace the Voice Gateway Media Card when the card is removed or when the following conditions occur:

- If the Voice Gateway Media Card displays a code of the form F:xx on the faceplate LED following a reboot, this indicates an unrecoverable hardware failure. The card cannot register with the Meridian 1 and Succession CSE 1000. The exception is the F:10 code, that can indicate that the Security Device is missing from the card.
- If the management Ethernet interface or the voice Ethernet interface on the Voice Gateway Media Card has failed. This can be indicated by failing to show a link pulse on the voice IP interface status LED or on the switch. It can also be indicated if the maintenance port continuously prints ‘lnIsa0 Carrier Failure’ messages after proving that the hub or switch port and ELAN cable are good.
- If a voice channel on the Voice Gateway Media Card has a consistent voice quality fault. For example, persistent noise or lack of voice path, even after resetting the card and retransmitting the card properties.

To replace a Voice Gateway Media Card, follow the steps in Procedure 93 on page 599.

> **CAUTION — Service Interruption**
>
> This procedure in this chapter are not supported for a node which resides on a Succession CSE 1000 Rel 2.0 system.

Procedure 93
Replacing a Voice Gateway Media Card

1 Locate the faulty card in the OTM ITG database by the TN, MAC address, and IP address.

2 Disable the faulty Voice Gateway Media Card in LD 32 with the **DISI** command. The Meridian 1 and Succession CSE 1000 outputs "NPR0011" when the card has been completely disabled by the DISI command.

3 Use the **disiTPS** command at the IPL> CLI to disable the TPS on the faulty Voice Gateway Media Card.

Note: This forces all Internet Telephones registered on this card to re-register. If there are sufficient resources, this can take up to several minutes. If there are not sufficient resources, Internet Telephones can remain unregistered indefinitely.

4 Use the **isetShow** command to monitor the status of the card and the reregistration of the Internet Telephones. The ITG Line card is completely disabled when there are no Internet Telephones registered on the card.

5 Remove the faulty Voice Gateway Media Card from the Meridian 1 and Succession CSE 1000.

6 In the **OTM Navigator**, select the **Services** folder. Double-click on the **ITG IP Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens. Select the node in the upper part of the window.

7 Click on Leader 0 or any Voice Gateway Media Card in the node.

8 Click **Configuration | Node | Properties**. The **ITG Node Properties** window opens.

9 Click the **Configuration** tab.

10 Select the card to be replaced.

11 Change the **Management MAC** to the MAC address of the replacement Voice Gateway Media Card. The MAC address is the Motherboard Ethernet address labeled on the faceplate of the replacement Voice Gateway Media Card.

12 Click **Change**, and then **OK**.

13 Select Leader 0 or any Voice Gateway Media Card in the node in the **IP Telephony Gateway - IP Line 3.0** window.

14 Use the **Configuration | Synchronize | Transmit**. The **ITG - Transmit Options** window opens.

15 Under **Transmit options**, select the **Transmit to Selected Nodes** radio button and check the **Node Properties to Active Leader** check box.

16 Click **Start transmit**. This updates the node properties on the active Leader card with the MAC Address of the replacement Voice Gateway Media Card. The results of the transmit displays under **Transmit control**. When the transmit is successful, click **Close**.

17 Install the replacement Voice Gateway Media Card into the card slots in the Meridian 1 IPE module/Option 11 cabinet or Succession CSE 1000 Media Gateway/Media Gateway Expansion. To do this:

a. Pull the top and bottom locking devices away from the card faceplate.

b. Insert the Voice Gateway Media Card into the card guides and gently push it until it makes contact with the backplane connector. Hook the locking devices.

Note 1: When cards are installed, the red LED on the faceplate remains lit until the card is configured and enabled in the software, at which point it turns off. If the LED does not follow the pattern described or operates in any other manner (such as continually flashing or remaining weakly lit), replace the card.

Note 2: Observe the faceplate maintenance display to see startup self-test results and status messages. A display of the type F:xx indicates a failure. Refer to Table 69 on page 553 for a listing of the ITG-P Line Card's display codes and to Table 70 on page 555 for a listing of the Succession Media Card's display codes.

18 In the OTM **IP Telephony Gateway- IP Line 3.0** window, select **View | Refresh** and verify that the replacement Voice Gateway Media Card state is showing "Unequipped."

End of Procedure

Verifying the Voice Gateway Media Card loadware and firmware

To verify the loadware on the Voice Gateway Media Card and the firmware on the Internet Telephone, follow the steps in Procedure 94.

> **CAUTION — Service Interruption**
>
> This procedure in this chapter are not supported for a node which resides on a Succession CSE 1000 Rel 2.0 system.

Procedure 94
Verifying the Voice Gateway Media Card loadware and firmware

Note: Refer also to Procedure 27, “Verifying card loadware and Internet Telephone firmware using OTM” on page 309.

1 Check the Nortel Networks Customer Support Web site for the latest IP Line loadware and Internet Telephone firmware releases. Download the **IP Line 3.00.xx SA** file. See Procedure 111 on page 719 for the steps for downloading files from the Nortel Networks Web site.

Note: The IP Line loadware and Internet Telephone firmware files are contained in the **IP Line 3.00.xx SA** file in the **Internet Telephony Gateway** product list on the Nortel Networks Web site.

The zip file contains:

- The **IPL300xx*.p2** and **IPL300xx*.sa** loadware files. The IPL300xx*.p2 file is the IP Line application for the ITG-P Line Card and the IPL300xx*.sa is the IP Line application for the Succession Media Card.
- The **0602Bxx.BIN** (i2004) firmware file.

  For example, a firmware version can be labelled 0602B38. This means Internet Telephone firmware version 1.38.

  — The 02 represents the i2004 Internet Telephone.

  — The letter B represents the Version number 1.

  — 38 represents the Release number .38.

- A **readme.txt** file. The readme.txt file explains important considerations for installing the new loadware and firmware versions. The readme file also includes identifying information for the loadware and firmware files such as the date and time, size and checksum.

2 Locate the saved file and double-click the *.zip file. The zipped file opens in a compression utility program and the uncompressed files are listed.

3 Compare the latest loadware and firmware versions available from the Nortel Networks Web site with the loadware and firmware version of the currently on the Voice Gateway Media Card.

a. In the **IP Telephony Gateway - IP Line 3.0** window, double-click the replacement Voice Gateway Media Card in the bottom of the window to open the **ITG Card Properties** window.

b. Leave the defaults in the Maintenance tab of the ITG Card Properties window. Click the **Configuration** tab.

c. Verify that the **S/W version** shows the latest recommended Voice Gateway Media Card loadware version. Verify that the **i2002 or i2004 F/W version** is the latest recommended release of the i2004 Internet Telephone firmware. Click **OK**.

4 If the card's loadware and firmware are not up-to-date, transfer the downloaded files (*.p2, *.sa, and firmware file(s)) from an Internet-enabled PC to the OTM PC.

5 Upgrade the loadware and/or firmware if required. Refer to "Upgrading Voice Gateway Media Card loadware from OTM PC" on page 314 and "Upgrading the Internet Telephone firmware" on page 318.

End of Procedure

Transmitting card properties

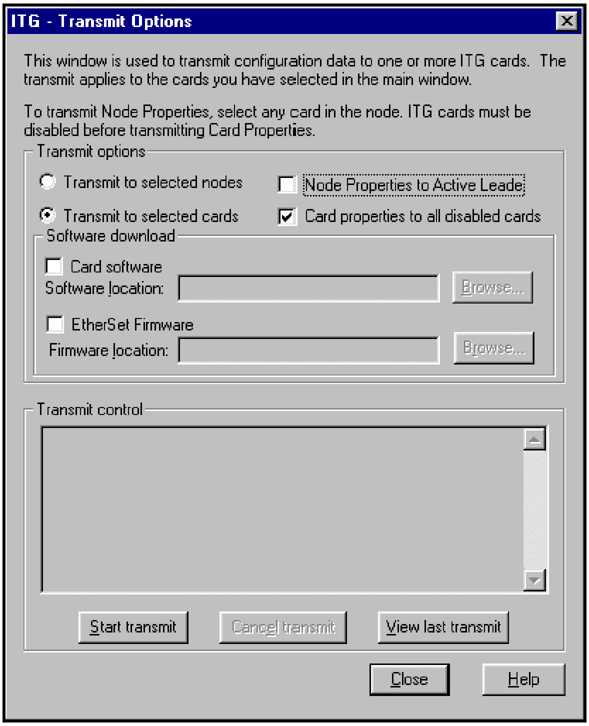
To transmit cards properties to the Voice Gateway Media Cards, follow the steps in Procedure 95.

> **CAUTION — Service Interruption**
>
> This procedure in this chapter are not supported for a node which resides on a Succession CSE 1000 Rel 2.0 system.

Procedure 95
Transmitting card properties

1. In the **OTM Navigator**, select the **Services** folder. Double-click on the **ITG Line 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.
2. Select the replacement Voice Gateway Media Card.
3. Click **Configuration** | **Synchronize** | **Transmit**.
4. The **ITG - Transmit Options** window opens (Figure 159 on page 604).

Figure 159
ITG Transmit Options dialog box



5 Select the **Transmit to selected cards** radio button. Check the **Card properties to all disabled cards** check box.

6 Click the **Start transmit** button.

The transmission status is displayed under **Transmit control**. Confirm that Card Properties are transmitted successfully.

7 When the transmission is successful, click **Close**.

8 Use the LD 32 **ENLC** command to re-enable the Voice Gateway Media Card.

9 Verify that the card is enabled in the **IP Telephony Gateway - IP Line 3.0**. Locate the card in the list at the bottom of the screen. Look under the **Card state** column and verify the card is **Enabled**.

10 Update the Installation Summary Sheet with the new MAC address (see “Voice Gateway Media Card installation summary sheet” on page 208).

11 Verify the TN, management interface MAC address, and IP address for each Voice Gateway Media Card. Compare the displayed values with those on the ITG Installation Summary Sheet.

End of Procedure

Accessing the IPL> Command Line Interface from OTM

To access the IPL> CLI from OTM, follow the steps in Procedure 74, “Accessing a Voice Gateway Media Card using Telnet” on page 494.

Adding a “dummy” node for retrieving and viewing IP Telephony node configuration

Use this procedure to create a “dummy” IP Telephony node for retrieving and viewing the IP Telephony node configuration, without overwriting the existing IP Line configuration data for an existing node in the OTM IP Line database.

Retrieving the actual IP Telephony node configuration to the “dummy” node is useful in the following cases:

- to isolate IP Telephony node configuration faults
- to determine which copy of the database is correct, in order to determine the desired direction of database synchronization:
  - transmit OTM IP Line to IP Telephony node, or
  - retrieve IP Telephony node to OTM IP Line.

The dummy node can be added manually or by retrieving the IP Telephony node configuration data from an existing node.

The site name, Meridian 1 and Succession CSE 1000 system name, and Meridian 1 and Succession CSE 1000 customer number must exist in the OTM Navigator before you can add a new IP Telephony node.

Procedure 96 is the recommended method to create the "dummy" IP Telephony node.

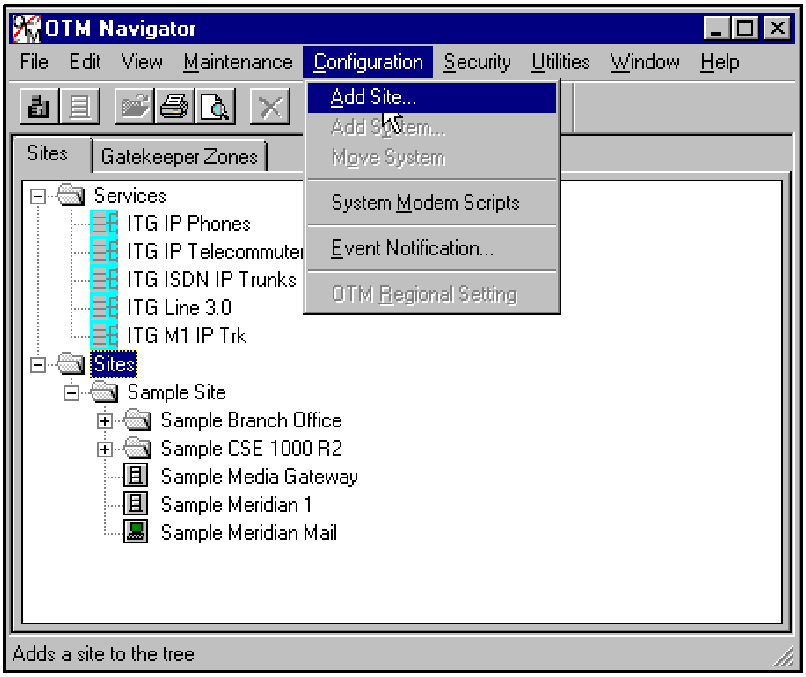
CAUTION — Service Interruption

This procedure in this chapter are not supported for a node which resides on a Succession CSE 1000 Rel 2.0 system.

Procedure 96
Creating the “dummy” IP Telephony node to retrieve configuration

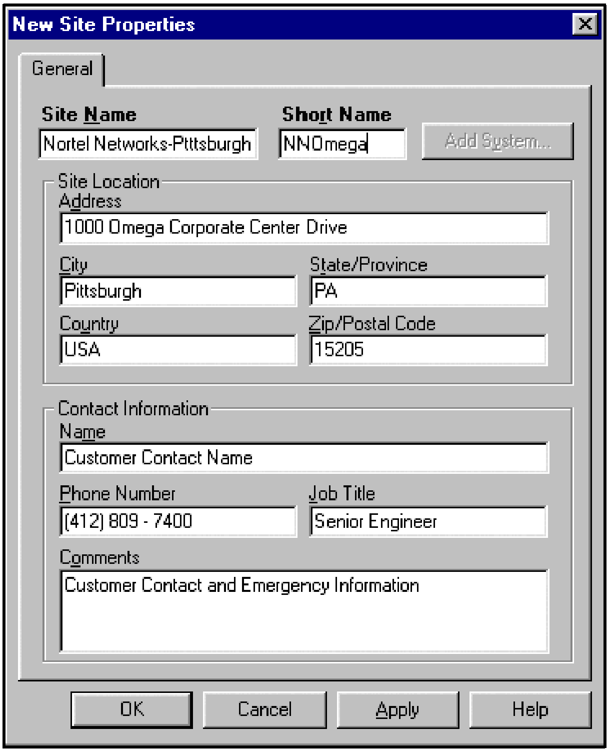
1 In **OTM Navigator**, click **Configuration | Add Site** (see Figure 160 on page 606).

Figure 160
OTM Navigator–Configuration | Add Site



2 The **New Site Properties** window opens (see Figure 161 on page 607).

Figure 161
New Site Properties



In the **New Site Properties** window, set the following:

a. **Site Name:** Add a site named "Retrieve ITG data."

b. **Short Name:** Enter a short name for the site.

Under **Site Location**, add the **Address**, **City**, **State/Province**, **Country**, and **Zip/Postal Code** of the site.

Under **Contact Information**, add the **Name**, **Phone Number**, **Job Title**, and any **Comments** for the site contact person(s).

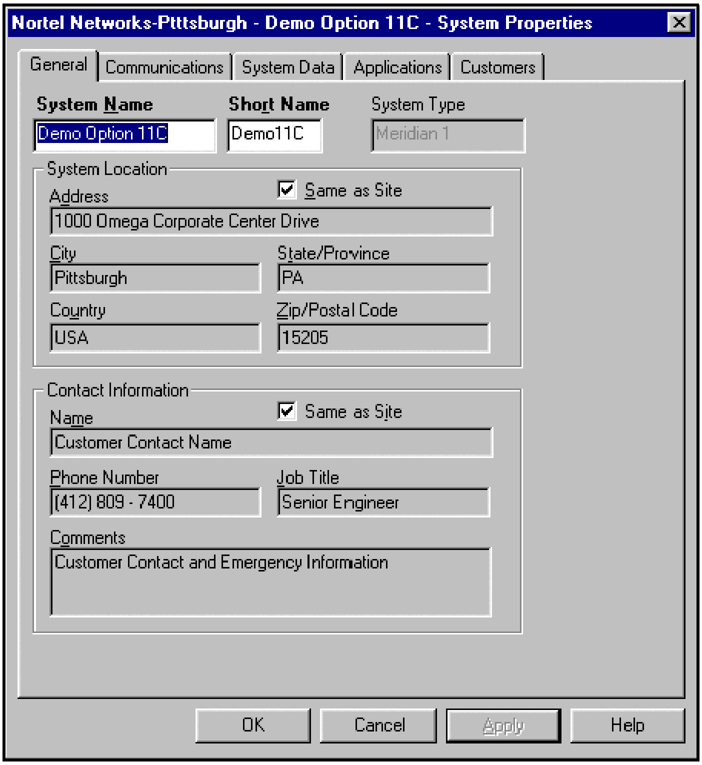
3 Click **Apply**, and then **OK**.

4 In **OTM Navigator**, click **Configuration | Add System**. The **Add System** window opens.

5 Add a system named “Dummy,” of type “Meridian 1,” under the site named “Retrieve ITG data.”

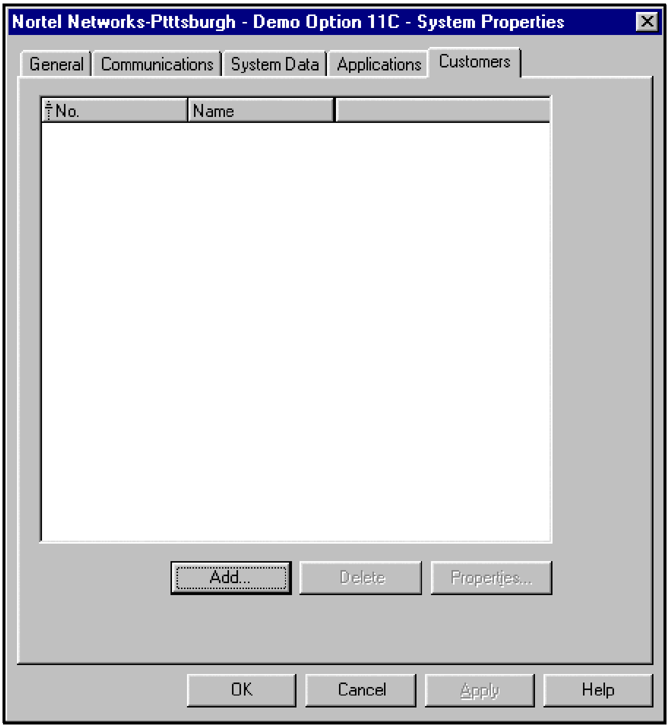
Under System Type, click **Meridian 1**, and then click **OK**. The **<Your Site> - System Properties** window opens (see Figure 162 on page 608).

Figure 162
System Properties–General Tab



6 Click the **Customers** tab (see Figure 163 on page 609).

Figure 163
System Properties–Customers tab



7 Click **Add**. Add Customer Number “99” on the “dummy” Meridian 1 system.

End of Procedure

Retrieving IP Line configuration from the IP Telephony node

Procedure 97 on page 610 is an optional procedure that can be used in the following cases:

- when adding an IP Telephony node on OTM by retrieving an existing node
- when you suspect that the IP Telephony node configuration on the Voice Gateway Media Card differs from the OTM IP Line database (for example, during maintenance and fault isolation procedures)

when you have multiple OTM IP Line PCs with multiple instances of the database (administration)

CAUTION — Service Interruption

This procedure in this chapter are not supported for a node which resides on a Succession CSE 1000 Rel 2.0 system.

Procedure 97
Retrieving IP Line configuration data from the IP Telephony node

Use the OTM IP Line **Configuration | Synchronize | Retrieve** command to retrieve the IP Line configuration information from the IP Telephony node.

1. In the **OTM Navigator**, select the **Services** folder and then double-click on the **ITG LIne 3.0** icon. The **IP Telephony Gateway - IP Line 3.0** window opens.
2. Select Leader 0 or any card from the node.
3. In the **IP Telephony Gateway - IP Line 3.0** window, click the **Configuration | Synchronize | Retrieve**.

   The **ITG - Retrieve Options** window opens.

4 Leave the defaulted "Node Properties" option selected, or click the "Card Properties," depending upon the situation:

  a. Leave the defaulted "Node Properties" when:

  — the OTM IP Line data is out of date and you intend to synchronize all OTM IP Telephony node data with the data from the Voice Gateway Media Cards on the node

  — adding a node in OTM by retrieving from an existing node that consists of more than one card

  b. Select "Card Properties" when you are attempting to isolate a problem with IP Line configuration on a particular card.

5 Select the check boxes for the IP Line configuration data that you want to retrieve, depending on the situation:

  a. Select **Node Properties** and **Card Properties**, if the OTM IP Line data is out of date and you intend to synchronize all OTM IP Telephony node data with the data from the Voice Gateway Media Cards on the node.

  b. Select **Card Properties** if you are adding a node on OTM by retrieving from an existing node that consists of more than one card.

  c. Select any combination of check boxes as indicated by problem symptoms when you are attempting to isolate a problem on a particular card. Use the "dummy" node for this purpose.

6 Click the **Start retrieve** button.

7 Monitor the progress of the retrieval under **Retrieve control** box.

The retrieved Node Properties and Card Properties overwrite the existing OTM IP Line configuration data for the respective node or card.

The "Retrieving the IP Line configuration information from the IP Telephony node" procedure is complete.

End of Procedure

Voice Gateway Media Card Maintenance using Element Management

Contents

This section contains information on the following topics:

Reference list

The following are references for this section:

- *Element Management* (553-3023-222)

Overview

This chapter provides information about the maintenance functions for the Succession Communication Server for Enterprise (CSE) 1000 Release 2.0 Voice Gateway Media Card.

Replacing a Voice Gateway Media Card

Replace the Voice Gateway Media Card when the card is removed or when the following conditions occur:

- If the Voice Gateway Media Card displays a code of the form F:xx on the faceplate LED following a reboot, this indicates an unrecoverable hardware failure. The card cannot register with the Succession CSE 1000 Rel 2.0 system. The exception is the F:10 code, that can indicate that the Security Device is missing from the card.
- If the management Ethernet interface or the voice Ethernet interface on the Voice Gateway Media Card has failed. This can be indicated by failing to show a link pulse on the voice IP interface status LED or on the switch. It can also be indicated if the maintenance port continuously prints 'lnIsa0 Carrier Failure' messages after proving that the hub or switch port and ELAN cable are good.
- If a voice channel on the Voice Gateway Media Card has a consistent voice quality fault, such as persistent noise or lack of voice path, even after resetting the card and retransmitting the card properties.

Replacing a Follower Voice Gateway Media Card

To replace a Follower Voice Gateway Media Card, follow the steps in Procedure 98 on page 614.

Procedure 98
Replacing a Follower Voice Gateway Media Card

1. Locate the faulty card by the TN, MAC address, and IP address.
2. Disable the faulty Voice Gateway Media Card in LD 32 with the **DISI** command. The Succession CSE 1000 Rel 2.0 system outputs "NPR0011" when the card has been completely disabled by the DISI command.
3. Use the **disiTPS** command at the IPL> CLI to disable the TPS on the faulty Voice Gateway Media Card.

   Note: This forces all Internet Telephones registered on this card to re-register. If there are sufficient resources, this can take up to several minutes. If there are not sufficient resources, Internet Telephones can remain unregistered indefinitely.

4 Use the **isetShow** command to monitor the status of the card and the reregistration of the Internet Telephones. The Voice Gateway Media card is completely disabled when there are no Internet Telephones registered on the card.

5 Remove the faulty Voice Gateway Media Card from the Succession CSE 1000 Rel 2.0 system.

6 Install the replacement Voice Gateway Media Card into the card slot in the Succession CSE 1000 Rel 2.0 Media Gateway/Media Gateway Expansion. To do this:

a. Pull the top and bottom locking devices away from the card faceplate.

b. Insert the Voice Gateway Media Card into the card guides and gently push it until it makes contact with the backplane connector. Hook the locking devices.

Note 1: When cards are installed, the red LED on the faceplate remains lit until the card is configured and enabled in the software, at which point it turns off. If the LED does not follow the pattern described or operates in any other manner (such as continually flashing or remaining weakly lit), replace the card.

Note 2: Observe the faceplate maintenance display to see startup self-test results and status messages. A display of the type F:xx indicates a failure. See Table 69 on page 553 for a listing of the ITG-P Line Card's display codes and to Table 70 on page 555 for a list of the Succession Media Card's display codes.

7 In Element Management, click **Configuration** in the Navigation Tree.

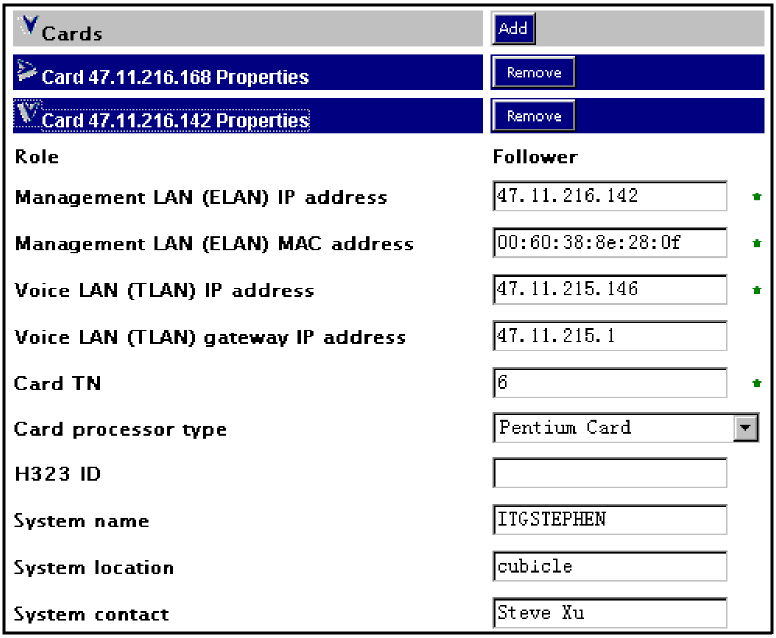
8 In the Configuration menu, click **IP Telephony**. The **Node Summary** page appears.

9 Click the **Edit** button associated with the node containing the card to be replaced. The **Edit** page appears.

10 Expand the **Cards** section.

11 Select the Voice Gateway Media Card from the list of cards in the node (see Figure 164 on page 616).

Figure 164
Cards



12 Change the **Management LAN (ELAN) MAC address** field to the MAC address of the replacement Voice Gateway Media Card. The MAC address is the Motherboard Ethernet address labeled on the faceplate of the replacement Voice Gateway Media Card.

13 Click **Submit**. The Node Summary pages opens.

14 Click the **Transfer** button associated with the node containing the Voice Gateway Media Card.

15 After the transfer is complete, restart the new card. Restarting the card, causes the follower card to obtains its BOOTP parameters from the Leader, and also establishes ELAN and TLAN connectivity.

16 Follow Procedure 45 on page 375 to load the CONFIG.INI file to the card.

17 Follow Procedure 50 on page 389 to download the latest loadware to the Voice Gateway Media Card.

18 Follow Procedure 51 on page 393 to reboot the card and run the new loadware.

19 Follow Procedure 52 on page 394 to update the card's firmware.

End of Procedure

Replacing a Leader Voice Gateway Media Card

To replace a Leader Voice Gateway Media Card, follow the steps in Procedure 99 on page 617.

Procedure 99
Replacing a Leader Voice Gateway Media Card

1 Locate the faulty card by the TN, MAC address, and IP address.

2 Disable the faulty Voice Gateway Media Card in LD 32 with the **DISI** command. The Succession CSE 1000 Rel 2.0 system outputs "NPR0011" when the card has been completely disabled by the DISI command.

3 Use the **disiTPS** command at the IPL> CLI to disable the TPS on the faulty Voice Gateway Media Card.

Note: This forces all Internet Telephones registered on this card to re-register. If there are sufficient resources, this can take up to several minutes. If there are not sufficient resources, Internet Telephones can remain unregistered indefinitely.

4 Use the **isetShow** command to monitor the status of the card and the reregistration of the Internet Telephones. The Voice Gateway Media Card is completely disabled when there are no Internet Telephones registered on the card.

5 Remove the faulty Voice Gateway Media Card from the Succession CSE 1000 Rel 2.0 system.

6 Install the replacement Voice Gateway Media Card into the card slot in the Succession CSE 1000 Rel 2.0 Media Gateway/Media Gateway Expansion. To do this:

a. Pull the top and bottom locking devices away from the card faceplate.

b. Insert the Voice Gateway Media Card into the card guides and gently push it until it makes contact with the backplane connector. Hook the locking devices.

Note 1: When cards are installed, the red LED on the faceplate remains lit until the card is configured and enabled in the software, at which point in turns off. If the LED does not follow the pattern described or operates in any other manner (such as continually flashing or remaining weakly lit), replace the card.

Note 2: Observe the faceplate maintenance display to see startup self-test results and status messages. A display of the type F:xx indicates a failure. Refer to Table 69 on page 553 for a listing of the ITG-P Line Card's display codes and to Table 70 on page 555 for a listing of the Succession Media Card's display codes.

7 Go to the VxWorks shell. Set the Voice Gateway Media Card as a Leader using the ELAN IP address and subnet mask.

8 Restart the card. The card gets the ELAN IP address and subnet mask.

9 In Element Management, click **Configuration** in the Navigation Tree.

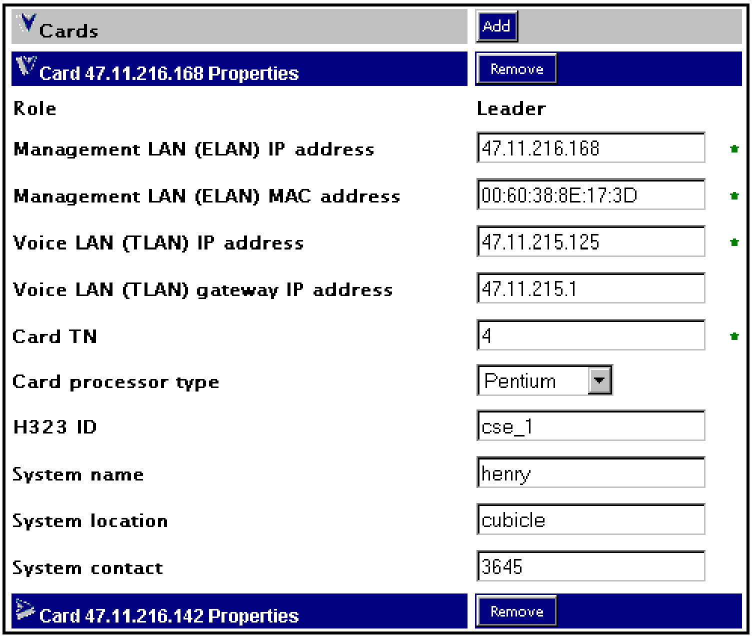
10 In the Configuration menu, click **IP Telephony**. The **Node Summary** page appears.

11 Click the **Edit** button associated with the node containing the card to be replaced. The **Edit** page opens.

12 Expand the **Cards** section.

13 Select the Voice Gateway Media Card from the list of cards in the node (see Figure 164 on page 616).

Figure 165
Cards



14 Change the **Management LAN (ELAN) MAC address** field to the MAC address of the replacement Voice Gateway Media Card. The MAC address is the Motherboard Ethernet address labeled on the faceplate of the replacement Voice Gateway Media Card.

15 Follow Procedure 44 on page 372 to load the CONFIG.INI file to the card.

16 Follow Procedure 50 on page 389 to download the latest loadware to the Voice Gateway Media Card.

17 Follow Procedure 51 on page 393 to reboot the card and run the new loadware.

18 Follow Procedure 52 on page 394 to update the card's firmware.

End of Procedure

Verifying Voice Gateway Media Card loadware and firmware

Refer to the following steps to verify and upgrade the loadware on the Voice Gateway Media Card and the firmware on the Internet Telephones.

The following steps are required to upgrade the card loadware and telephone firmware:

1 Check the version of the loadware currently installed on the Voice Gateway Media Card. Refer to Procedure 46 on page 381.

2 Check the version of the firmware that is currently running on the Voice Gateway Media Card. Refer to Procedure 47 on page 383.

3 Download the most up-to-date version of the loadware and firmware files from the Nortel Networks Web site. Refer to Procedure 48 on page 386.

4 Upload the loadware and firmware files using the File Upload system utility in Element Management. Refer to Procedure 49 on page 388.

5 Upgrade the Voice Gateway Media Card loadware. Refer to Procedure 50 on page 389.

6 Restart the Voice Gateway Media Card. Refer to Procedure 51 on page 393.

7 Upgrade and distribute the firmware to the Internet Telephones on the Voice Gateway Media Card. Refer to Procedure 52 on page 394.

Accessing the CLI commands within Element Management

The following list of informational CLI commands are available from Element Management:

Voice Gateway Media Card CLI Commands

- cardRoleShow
- disiAll
- disiTPS
- dspSWVersionShow
- DSPNumShow
- electShow
- i
- ifShow
- IPInfoShow
- ipstatShow
- isetShow
- itgCardShow
- nodePwdDisable
- nodePwdEnable
- nodePwdShow
- nodeTempPwdClear
- pbxLinkShow
- routeShow
- rudpShow
- umsPolicyShow
- ping
- nodePwdSet
- nodeTempPwdSet

Signaling Server CLI Commands

- cardRoleShow
- disiAll
- disiTPS
- electShow
- i
- ifShow
- IPInfoShow
- ipstatShow
- isetShow
- itgCardShow
- nodePwdDisable
- nodePwdEnable
- nodePwdShow
- nodeTempPwdClear
- pbxLinkShow
- routeShow
- rudpShow
- umsPolicyShow
- ping
- nodePwdSet
- nodeTempPwdSet

Refer to "IP Line CLI commands" on page 567 for descriptions of these commands.

To access these commands in Element Management, follow the steps in Procedure 100 on page 622.

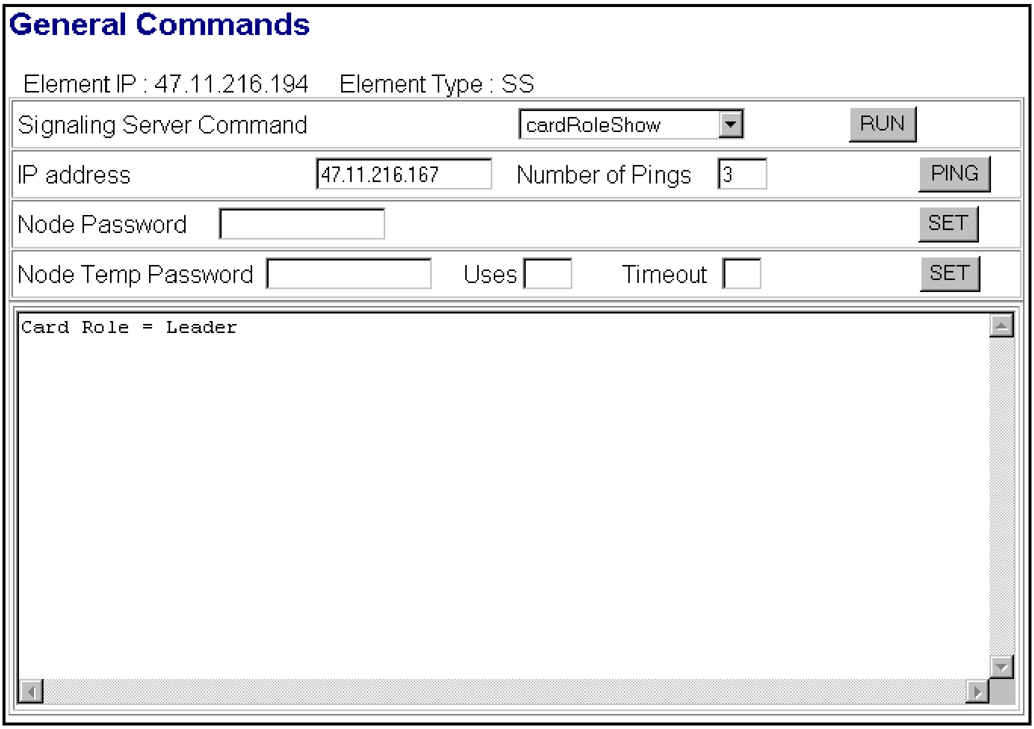
Procedure 100
Accessing the CLI commands from Element Management

1 Select **System Status** and then **IP Telephony** from the Navigation Tree. The IP Telephony Information pages opens.

2 Expand the node containing the Voice Gateway Media Card.

3 Click the **GEN CMD** button associated with the Voice Gateway Media Card. The **General Commands** page opens (see Figure 166 on page 622).

Figure 166
System Status > IP Telephony > GEN CMD button > General Commands



Note: The first section shown on the top of the General Commands page is **ITGL Commands** or **Signaling Server Command**. The section displayed depends on whether a card or Signaling Server was selected in the IP Telephony Information page.

4 In the ITGL Commands (or Signaling Server Command) section, select the CLI command from the drop-down list box and click **RUN**.

The output of the command is displayed in the text area at the bottom of the General Commands page.

End of Procedure

Sample Output of Element Management CLI commands

cardRoleShow

Card Role = Follower

disiAll

There is no output or message returned in the text area from the disiAll command.

disiTPS

There is no output or message returned in the text area from the disiTPS command.

dspSWVersionShow

DSP software version R8.01

DSPNumShow

Number of DSPs = 8

electShow

Node ID: 444
Is master: 0
Up Time(sec): 219612
TN: 080c
Platform: ITG SA
IP TLAN: 47.104.39.243
IP ELAN: 47.104.39.115
Election Duration: 2
Wait for Result time: 125
Master Broadcast period: 120

master tps

PlatForm TN TLAN
ISP 1100 0000 47.104.39.245
Next timeout = 71 sec
AutoAnnounce: 1
Timer duration : 60 (Next timeout in 25 sec)

all tps

Num	Platform	TN	TLAN	ELAN	TimeOut
0	ITG SA	080c	47.104.39.243	47.104.39.115	0
1	ISP 1100	0000	47.104.39.246	47.104.39.118	0
2	ISP 1100	0000	47.104.39.245	47.104.39.117	0
3	ITG SA	0c04	47.104.39.244	47.104.39.116	1

i

NAME	ENTRY	TID	PRI	STATUS	PC	SP	ERRNO	DELAY
tExcTask	_excTask	339a824	0	PEND	2aca80	339a758	3006b	0
tShell	_shell	2e31e30	1	PEND	231e08	2e316d4	0	0
...	...	...	...	...	...	...	...	...
tSET	19be9c	2b6263c	200	PEND	256d84	2b62518	320001	0
tSyslogd	10a58	3aff168	255	READY	22f6d0	3afeac4	0	0

ifShow

```
ixpMac (unit number 1):
Flags: (0x8863) UP BROADCAST MULTICAST ARP RUNNING
Type: ETHERNET_CSMACD
Internet address: 47.104.39.115
Broadcast address: 47.104.39.127
Netmask 0xff000000 Subnetmask 0xffffff80
Ethernet address is 00:60:38:bd:bb:cd
Metric is 0
Maximum Transfer Unit size is 1500
298604 packets received; 23909 packets sent
278631 multicast packets received
4608 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
lo (unit number 0):
Flags: (0x8069) UP LOOPBACK MULTICAST ARP RUNNING
Type: SOFTWARE_LOOPBACK
Internet address: 127.0.0.1
Netmask 0xff000000 Subnetmask 0xff000000
Metric is 0
Maximum Transfer Unit size is 32768
4 packets received; 4 packets sent
0 multicast packets received
0 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
ixpMac (unit number 0):
Flags: (0x8863) UP BROADCAST MULTICAST ARP RUNNING
Type: ETHERNET_CSMACD
Internet address: 47.104.39.243
Broadcast address: 47.104.39.255
Netmask 0xff000000 Subnetmask 0xffffff80
Ethernet address is 00:60:38:bd:bb:cc
Metric is 0
Maximum Transfer Unit size is 1500
88686 packets received; 15027 packets sent
78030 multicast packets received
5044 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
```

IPInfoShow

Maintenance Interface = ixpMac1
Maintenance IP address = 47.104.39.115
Maintenance subnet mask = 255.255.255.128
Voice Interface = ixpMac0
Voice IP address = 47.104.39.243
Voice subnet mask = 255.255.255.128

ROUTE NET TABLE

destination	gateway	flags	Refcnt	Use	Interface
0.0.0.0	47.104.39.129	3	0	675	ixpMac0
47.104.39.0	47.104.39.115	101	0	0	ixpMac1
47.104.39.128	47.104.39.243	101	0	0	ixpMac0

ROUTE HOST TABLE

destination	gateway	flags	Refcnt	Use	Interface
127.0.0.1	127.0.0.1	5	0	0	lo0

ipstatShow

total 128099
badsum 0
tooshort 0
toosmall 0
badhlen 0
badlen 0
infragments 0
fragdropped 0
fragtimeout 0
forward 0
cantforward 486
redirectsent 0
unknownprotocol 0
nobuffers 0
reassembled 0
outfragments 0
noroute 0

isetShow

No sets registered

itgCardShow

Index: 3
Type: EXUT
Role: Follower
Node: 444
Leader IP: 47.104.39.240
Card IP: 47.104.39.243
Card TN: Slot 11
Card State: ENBL
Uptime: 1 days, 19 hours, 36 mins, 17 secs (156977 secs)
Codecs: G711Ulaw(default), G711Alaw, G729A, G729AB, G711CC, T38FAX
lnPci stat: 100 Mbps (Carrier OK)

nodePasswordDisable

Please run nodePwdShow to verify the result.
Run nodePwdShow and get the following results:

NodeID	PwdEna	Pwd	TmpPwd	Uses	TimeOut
======	=======	====	=======	====	========
444	No			0	0d 0h 0m 0s

nodePasswordEnable

Please run nodePwdShow to verify the result.

Run nodePwdShow and get the following results:

NodeID	PwdEna	Pwd	TmpPwd	Uses	TimeOut
======	=======	====	=======	====	========
444	No			0	0d 0h 0m 0s

nodePasswordShow

NodeID	PwdEna	Pwd	TmpPwd	Uses	TimeOut
======	=======	====	=======	====	========
444	No			0	0d 0h 0m 0s

nodeTempPwdClear

Please run nodePwdShow to verify the result.

Run nodePwdShow and get the following results:

NodeID	PwdEna	Pwd	TmpPwd	Uses	TimeOut
======	=======	====	=======	====	========
444	No			0	0d 0h 0m 0s

pbxLinkShow

Active CS type = Succession CSE 1K
Active CS S/W Release = 201R
Supported Features: GetCSVsn TCP ShiftKey I2050 I2002 CorpDir UserKeyLabel VirtualOffice UseCSPwd
CS Main: ip = 47.104.39.112, ConnectID = 0x2bbfb4c, BroadcastID = 0x2bc059c, Link is up
CS Signaling Port = 15000
CS Broadcast Port = 15001
Broadcast PortID = 0x2bc06fc
RUDP portID = 0x2bc0684
Tcp Link state = up
Tcp Signaling Port: 15000
Tcp socket fd: 30
Tcp msgs sent: 77
Tcp msgs recd: 47

routeShow

ROUTE NET TABLE

destination	gateway	flags	Refcnt	Use	Interface
0.0.0.0	47.104.39.129	3	0	675	ixpMac0
47.104.39.0	47.104.39.115	101	0	0	ixpMac1
47.104.39.128	47.104.39.243	101	0	0	ixpMac0

ROUTE HOST TABLE

destination	gateway	flags	Refcnt	Use	Interface
127.0.0.1	127.0.0.1	5	0	0	lo0

rudpdShow

RUDP Port Summary

Port ID +--------------+	Src IP -----------------+	Src Port ----------+
0x02bc06fc	0.0.0.0	15001
0x02bc0684	47.104.39.115	15000
0x02b563cc	47.104.39.243	7300
0x02321ad0	47.104.39.243	5100

RUDP Connection Summary

Src IP +-------------+	Src Port ------+	Connect ID ----------+	Dst IP ----------------+	Dst Port ------+	Status --------+	Msg rcv ----+	Msg sent -----+	Retries -------+
0.0.0.0	15001	0x02bc059c	47.104.39.112	15000	DUDP	0	0	0
47.104.39.115	15000	0x02bbfb4c	47.104.39.112	15000	ESTABLISHED <->	1	2628	1

umsPolicyShow

Total firmware = 2

FirmWare	TermType	PolicyName	Server	FileName	Limit	When	Upgrade	Protocol	Retry
0602B38	i2004	DEFAULT _I2004	47.104.39.243	/ums/i2004.fw	10	ALWAYS	ANY	TFTP	-1
0603B38	i2002	DEFAULT _I2002	47.104.39.245	/ums/i2002.fw	10	ALWAYS	ANY	TFTP	-1

vgwShowAll

VGW Service is: Enabled

Chan	ChanState	DspMode	Codec	Tn	Reg	AirTime	rxTsap	txTsap
0	Idle	Closed	n/a	0x080c	yes	0	0.0.0.0:0000	0.0.0.0:0000
1	Idle	Closed	n/a	0x080d	yes	0	0.0.0.0:0000	0.0.0.0:0000
2	Idle	Closed	n/a	0x080e	yes	0	0.0.0.0:0000	0.0.0.0:0000
3	Idle	Closed	n/a	0x080f	yes	0	0.0.0.0:0000	0.0.0.0:0000
4	Idle	Closed	n/a	0x084c	yes	0	0.0.0.0:0000	0.0.0.0:0000
5	Idle	Closed	n/a	0x084d	yes	0	0.0.0.0:0000	0.0.0.0:0000
6	Idle	Closed	n/a	0x084e	yes	0	0.0.0.0:0000	0.0.0.0:0000
7	Idle	Closed	n/a	0x084f	yes	0	0.0.0.0:0000	0.0.0.0:0000
8	Idle	Closed	n/a	0x088c	yes	0	0.0.0.0:0000	0.0.0.0:0000
9	Idle	Closed	n/a	0x088d	yes	0	0.0.0.0:0000	0.0.0.0:0000
10	Idle	Closed	n/a	0x088e	yes	0	0.0.0.0:0000	0.0.0.0:0000
11	Idle	Closed	n/a	0x088f	yes	0	0.0.0.0:0000	0.0.0.0:0000
12	Idle	Closed	n/a	0x08cc	yes	0	0.0.0.0:0000	0.0.0.0:0000
13	Idle	Closed	n/a	0x08cd	yes	0	0.0.0.0:0000	0.0.0.0:0000
14	Idle	Closed	n/a	0x08ce	yes	0	0.0.0.0:0000	0.0.0.0:0000
15	Idle	Closed	n/a	0x08cf	yes	0	0.0.0.0:0000	0.0.0.0:0000
16	Idle	Closed	n/a	0x090c	yes	0	0.0.0.0:0000	0.0.0.0:0000
17	Idle	Closed	n/a	0x090d	yes	0	0.0.0.0:0000	0.0.0.0:0000
18	Idle	Closed	n/a	0x090e	yes	0	0.0.0.0:0000	0.0.0.0:0000
19	Idle	Closed	n/a	0x090f	yes	0	0.0.0.0:0000	0.0.0.0:0000
20	Idle	Closed	n/a	0x094c	yes	0	0.0.0.0:0000	0.0.0.0:0000
21	Idle	Closed	n/a	0x094d	yes	0	0.0.0.0:0000	0.0.0.0:0000
22	Idle	Closed	n/a	0x094e	yes	0	0.0.0.0:0000	0.0.0.0:0000
23	Idle	Closed	n/a	0x094f	yes	0	0.0.0.0:0000	0.0.0.0:0000
24	Idle	Closed	n/a	0x098c	yes	0	0.0.0.0:0000	0.0.0.0:0000
25	Idle	Closed	n/a	0x098d	yes	0	0.0.0.0:0000	0.0.0.0:0000
26	Idle	Closed	n/a	0x098e	yes	0	0.0.0.0:0000	0.0.0.0:0000
27	Idle	Closed	n/a	0x098f	yes	0	0.0.0.0:0000	0.0.0.0:0000
28	Idle	Closed	n/a	0x09cc	yes	0	0.0.0.0:0000	0.0.0.0:0000
29	Idle	Closed	n/a	0x09cd	yes	0	0.0.0.0:0000	0.0.0.0:0000
30	Idle	Closed	n/a	0x09ce	yes	0	0.0.0.0:0000	0.0.0.0:0000
31	Idle	Closed	n/a	0x09cf	yes	0	0.0.0.0:0000	0.0.0.0:0000

Access the IPL> Command Line Interface from Element Management

To access the IPL> CLI from with Element Management, follow the steps in Procedure 87, “Accessing a Voice Gateway Media Card using Telnet” on page 538.

Appendix A: I/O, Maintenance, and Extender Cable Description

Contents

This section contains information on the following topics:

Overview

This appendix describes the NTMF94EA, NTAG81CA, and NTAG81BA cables and explains how to replace the NT8D81BA backplane ribbon cable and install the NTCW84JA filter, if required.

NTMF94EA I/O cable

The NTMF94EAcable provides the ELAN and TLAN ports that provide the interface from the IP Line card to the customer's network equipment. This cable also has one DB9 serial port that provides serial connection between the card and the customer PC or TTY (see Figure 167 on page 635).

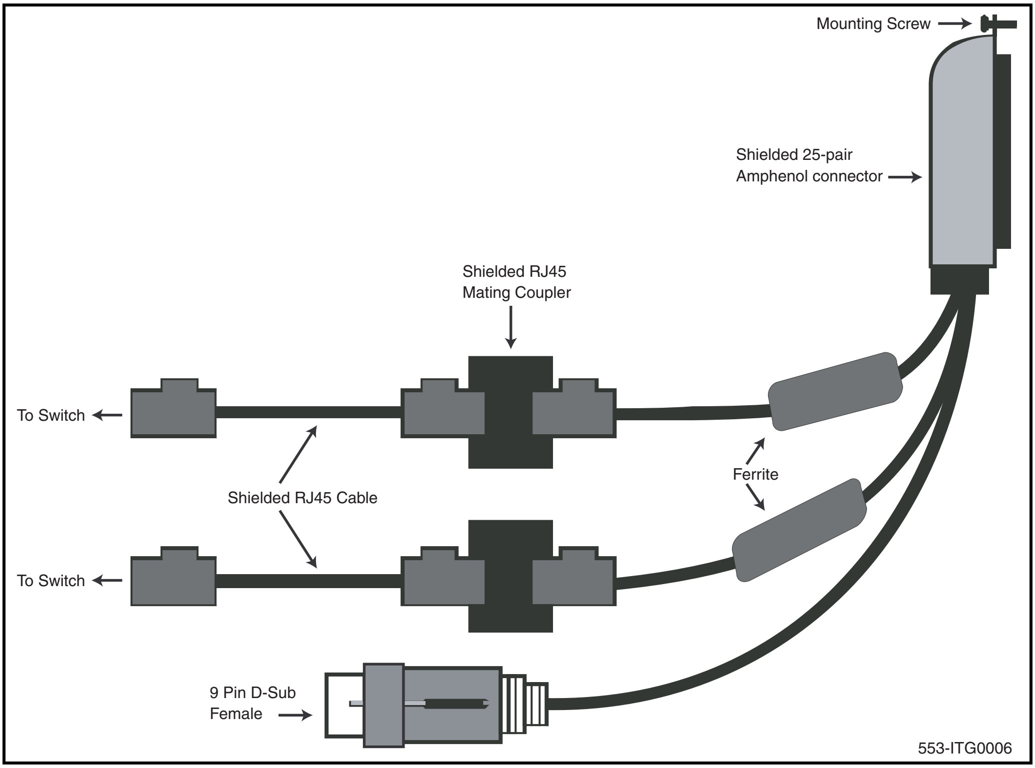
It is important to use the mounting screw provided to secure the top of the NTMF94EA cable 25-pair Amphenol connector to the Meridian 1 and Succession Communication Server for Enterprise 1000. The screw ties the LAN cable shield to the Meridian 1 and Succession CSE 1000 frame ground for EMC compliance.

The NTMF94EA cable provides a factory installed, shielded, RJ-45 to RJ-45 coupler at the end of both the ELAN and the TLAN ports. An unshielded coupler is provided to prevent ground loops (if required). Refer to "Prevent ground loops on connection to external customer LAN equipment" on page 638, to determine if you should use the unshielded coupler. Both ends of the RJ-45 ports of the cables are labeled to distinguish the TLAN and the ELAN. The ports provide the connection point to the customer's ELAN and TLAN equipment. You must use shielded Category 5 cable to connect to the customer's equipment.

To improve EMC performance, use standard cable ties to bundle all LAN cables as they route out of the system.

> ***Note:*** To avoid damage to Category 5 cable, do not overtighten cable ties.

Figure 167
NTMF94EA ELAN, TLAN and RS-232 Serial Maintenance I/O cable



Connector pin assignments

Table 91 shows the I/O connector pin designations for the Voice Gateway Media Card.

Table 91
Voice Gateway Media Card I/O Panel Pinout (Part 1 of 2)

Pin	Normal Assignment	ITG Assignment	Pin	Normal Assignment	ITG Assignment
2	R1	Not Used	26	T0	Not Used
3	R2	Not Used	27	T1	Not Used
4	R3	Not Used	28	T2	Not Used
5	R4	Not Used	29	T3	Not Used
6	R5	AGND	30	T4	AGND
7	R6	Not Used	31	T5	Not Used
8	R7	Not Used	32	T6	Not Used
9	R8	Not Used	33	T7	Not Used
10	R9	AGND	34	T8	AGND
11	R10	PGT0	35	T9	PGT1
12	R11	PGT2	36	T10	PGT3
13	R12	PGT4	37	T11	PGT5
14	R13	PGT6	38	T12	PGT7
15	R14	PGT8	39	T13	PGT9
16	R15	PGT10	40	T14	PGT11
17	R16	SGNDA	41	T15	BDCDA-
18	R17	BSINA-	42	T16	BSOUTA-
19	R18	BDTRA-	43	T17	SGND
20	R19	BDSRA-	44	T18	BRTSA-

Table 91
Voice Gateway Media Card I/O Panel Pinout (Part 2 of 2)

Pin	Normal Assignment	ITG Assignment	Pin	Normal Assignment	ITG Assignment
21	R20	BCTSA-	45	T19	BSINB-
22	R21	BSOUTB-	46	T20	BDCDB-
23	R22	BDTRB-	47	T21	BDSRB-
24	R23	DI+	48	T22	DI-
25	no connect	DO+	49	T23	DO-
2	R1	no connect	50	no connect	no connect

Table 92
NTMF94EA cable pin description (Part 1 of 2)

I/O Panel: P1	Signal Name	P2, P3,P4	Color
P1-21	BSOUTB-	P2-2	RED
P1-22	BDTRB-	P2-4	GREEN
	SGRND	P2-5	BROWN
P1-45	BSINB-	P2-3	BLUE
P1-46	BDCDB-	P2-1	ORANGE
P1-47	BDSRB-	P2-6	YELLOW
P1-25	SHLD GRND		
P1-50	SHLD GRND		
P1-18	RXDB+	P4-3	GREEN/WHITE
P1-19	TXDB+	P4-1	ORANGE/WHITE
P1-43	RXDB-	P4-6	WHITE/GREEN

Table 92
NTMF94EA cable pin description (Part 2 of 2)

I/O Panel: P1	Signal Name	P2, P3,P4	Color
P1-44	TXDB-	P4-2	WHITE/ORANGE
P1-23	RX+	P3-3	GREEN/WHITE
P1-24	TX+	P3-1	ORANGE/WHITE
P1-48	RX-	P3-6	WHITE/GREEN
P1-49	TX-	P3-2	WHITE/ORANGE
P1-25	SHLD GRND		BARE
P1-50	SHLD GRND		BARE

Prevent ground loops on connection to external customer LAN equipment

The shielded RJ-45 coupler is the connection point for the customer's shielded Category 5 LAN cable to the hub, switch, or router supporting the TLAN and ELAN. You must use shielded Category 5 RJ-45 cable to connect to the customer's TLAN/ELAN equipment.

1 Connect the customer-provided shielded Category 5 LAN cable to the external LAN equipment. Ensure that the external LAN equipment is powered-up.

2 Use an ohmmeter to measure resistance to ground between the free end of the shielded RJ-45 cable and the building ground.

The ohmmeter must measure Open to ground before plugging it into the shielded RJ-45 coupler on the end of the NTMF94EA.

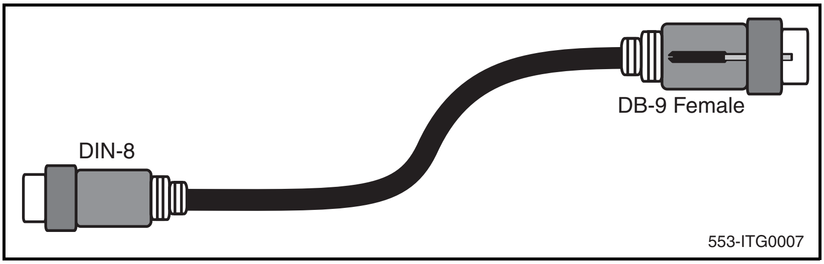
3 If the ohmmeter does not measure Open, you must install the unshielded RJ-45 coupler (provided) on the end of the NTMF94EA to prevent ground loops to external LAN equipment.

WARNING
The serial maintenance ports on the faceplate connector and the DB-9 female connector of the NTMF9DA cable assembly are identical. Do not connect a serial device to both access points simultaneously. This results in incorrect and unpredictable operation of the Voice Gateway Media Card.

NTAG81CA maintenance cable description

The NTAG81CA maintenance cable (see Figure 168 on page 639) is connected between the 9-pin D-type RS232 input on a standard PC and the MAINT connector on the NT8R17AB faceplate or through the I/O cable serial port.

Figure 168
NTAG81CA Maintenance cable



The NTAG91CA maintenance cable pin description is outlined in Table 93.

Table 93
NTAG81CA maintenance cable pin description

Signals (MIX Side)	8-pin Mini-DIN (MIX Side) Male	9-pin D-Sub (PC Side) Female	Signals (PC Side)
DTRB-	1	6	DSR-
SOUTB-	2	2	SIN-
SINB-	3	3	SOUT-
GND	4	5	GND
SINA-	5	nc	nc
CTSA-	6	nc	nc
SOUTA-	7	nc	nc
DTRA-	8	nc	nc

NTAG81BA maintenance extender cable

The NTAG81BA maintenance extender (3m) cable connects the NTAG81CA cable to a PC or terminal. It has a 9-pin D-type connector at both ends, one male and one female (see Table 94). It can also be used to extend the serial port presented by the NTMF94EA I/O panel cable. The extender cable is shown in Table 169 on page 641.

Table 94
NTAG81BA Maintenance cable pin description

9-pin D-Sub (Male)	9-pin D-Sub (Female)
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9

Figure 169
NTAG81BA Maintenance Extender cable

Replacing the NT8D81BA cable with the NT8D1AA cable and installing the NTCW84JW special IPE filter

This procedure explains how to replace the NT8D81BA cable with the NT8D81AA cable and how to install the NTCW84JA special IPE filter in the Meridian 1 IPE module.

Cables are designated by the letter of the I/O panel cutout, such as A, B, and C, where the 50-pin cable connector is attached. Each cable has three 20-pin connectors (16 positions are used), designated 1, 2, and 3, that attach to the backplane. Using the designations described, the backplane ends of the first cable are referred to as A-1, A-2, and A-3. The locations of the cable connectors on the backplane are designated by the slot number (L0 through L9 for NT8D11, L0 through L15 for NT8D37) and the shroud row (1, 2, and 3). Using these designations, the slot positions in the first slot are referred to as L0-1, L0-2, and L0-3.

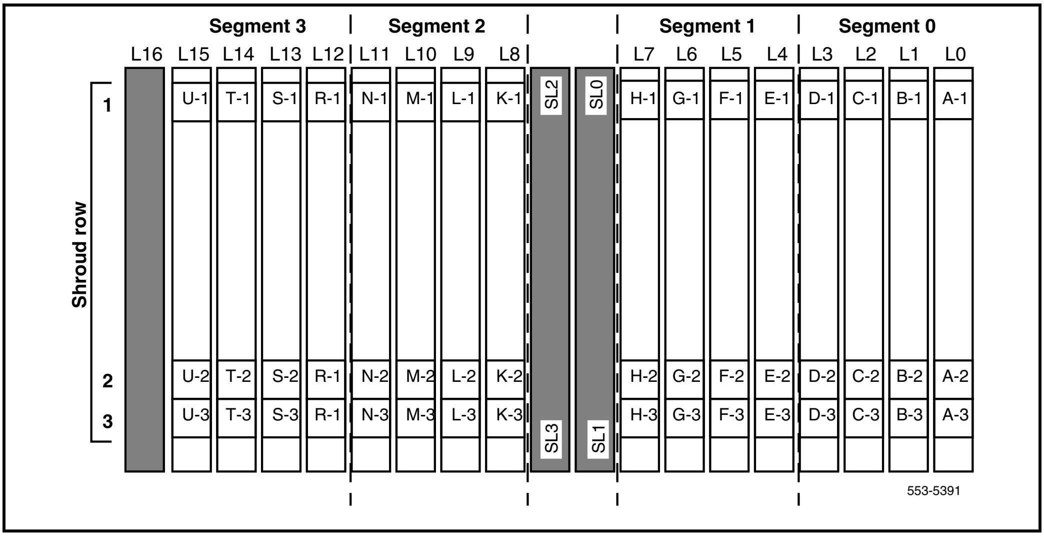
In NT8D37BA and NT8D37EC (and later vintage) IPE Modules, all 16 IPE card slots support 24-pair cable connections. Table 95: "NT8D37 cable connections" on page 643 shows the cable connections from the backplane to the inside of the I/O panel.

Table 95
NT8D37 cable connections

Backplane slots–shroud rows	I/O panel/cable designation
L0–1, 2, 3	A
L1–1, 2, 3	B
L2–1, 2, 3	C
L3–1, 2, 3	D
L4–1, 2, 3	E
L5–1, 2, 3	F
L6–1, 2, 3	G
L7–1, 2, 3	H
L8–1, 2, 3	K
L9–1, 2, 3	L
L10–1, 2, 3	M
L11–1, 2, 3	N
L12–1, 2, 3	R
L13–1, 2, 3	S
L14–1, 2, 3	T
L15–1, 2, 3	U

Figure 170 on page 644 shows the designations for the backplane end of the cables, the backplane slot designations for the cable connections, and the associated network segments for the backplane slots.

Figure 170
Backplane slot designations



Tools list

The following tools are required to perform this procedure.

- Ty-wrap cutter
- Ty-wraps
- Needle nose pliers
- Slotted screwdriver

Procedure 101
Removing an NT8D81BA cable

1 Identify the I/O panel and backplane designation that corresponds to the LEFT slot of the pair of card slots, viewed from the front, in which you installed the ITG ISL Trunk card.

2 Disconnect the filter from the I/O panel using a screwdriver and needle nose pliers. Retain the fasteners.

3 Power down the IPE shelf.

4 Remove the IPE module I/O safety panel.

5 To remove the ribbon cables from IPE backplane, apply gentle pressure on the tab on the right side of the shroud while pulling on the connector until it pulls free from the shroud.

Remove connector 1 first, then remove connectors 2 and 3.

6 Discard NT8D81BA cable.

End of Procedure

Procedure 102
Installing an NTCW84JA filter and NT8D81AA cable

1 Install NTCW84JA special IPE filter connector in the vacant I/O panel slot using retained hardware.

2 Install NT8D81AA ribbon cable connectors in the IPE module backplane shroud. Be sure to install the connector so the label is facing right with the arrow pointing up and the connector is fully engaged into the shroud:

a. Install connector 1, (labeled UP1^) into backplane shroud 1.

b. Install connector 2, (labeled UP2^) into backplane shroud 2.

c. Install connector 3, (labeled UP3^) into backplane shroud 3.

3 Dress the ribbon cables back individually inside the rear of IPE module and restore the original arrangement. Start with the cables that are going to be underneath.

4 Attach NTCW84JA special IPE filter to NT8D81AA 50-pin connector using bail clips.

5 Restore power to the IPE module.

6 Replace the I/O safety panel.

End of Procedure

Appendix B: RM356 Modem Router

Contents

This section contains information on the following topics:

Overview

Management and support of the IP Line network depend on IP networking protocols including SNMP, FTP, and Telnet. Install a modem router on the Meridian 1 and Succession Communication Server for Enterprise 1000 site LAN (called the embedded LAN or ELAN as opposed to the customer's enterprise network or CLAN) in order to provide remote support access for ITG and other IP-enabled Nortel Networks products.

WARNING
Nortel Networks strongly recommends that the RM356 modem router be installed for management and support.

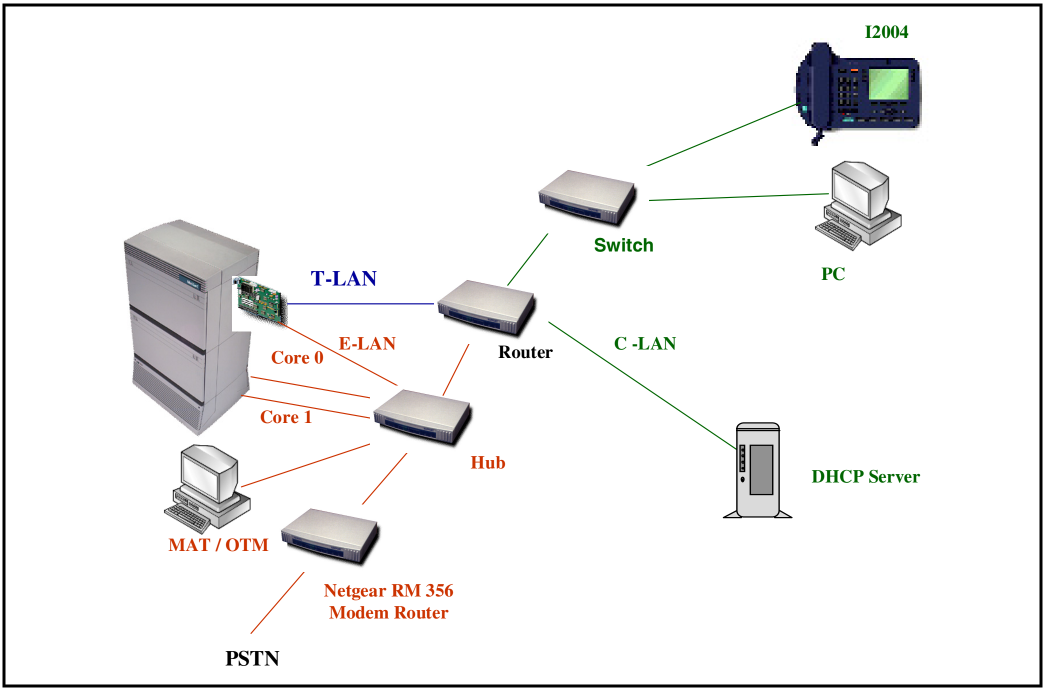
The Netgear RM356 modem router integrates the functions of a V.90 modem, a PPP remote access server, an IP router, and a 4-port 10BaseT Ethernet hub, and provides a range of security features configured to comply with the customer's data network security policy. Do not install a modem router on the ELAN without the explicit approval of the customer's IP network manager. The RM356 modem router is not secure unless it is configured correctly according to the customer's network security policy and practices. Figure 171 on page 649 shows an example of a remote network.

RM356 modem router security features

The security features of the RM356 modem router include:

- Password Authentication Protocol (PAP) for dial-in PPP connection
- RM356 manager password
- CLID for dial-in user authentication (requires C.O. line with Calling Line ID)
- Callback for dial-in user authentication
- Dial-in user profiles
- Static IP routing
- IP Packet Filtering
- Idle timeout disconnect for dial-in PPP connection

Figure 171
Remote support using Netgear RM356 modem router



Install the RM356 modem router

Procedure 103
Installing the RM356 modem router

1 Place the modem router at a conveniently visible and physically secure location near an AC power outlet, an analog telephone line, and a 10BaseT Ethernet cable.

Up to four hosts or hubs can be connected to the integrated 10BaseT hub in the rear of the RM356 modem router.

2 Use shielded Cat5 10BaseT Ethernet cables to connect the modem router to the ELAN switch. Other IP-enabled Nortel Networks products on the ELAN can be connected to the RM356 modem router, including the Meridian 1 PBX, Succession CSE 1000, a local Optivity Telephone Manager (OTM) 2.0 PC, Symposium Call Center Server, and Call Pilot.

Note: The up-link connection to an additional ELAN hub or optional gateway on the customer's enterprise network (CLAN) requires either a cross-over 10BaseT Ethernet cable or a special up-link port on the 10BaseT hub to which the RM356 is connected.

3 Connect the modem router to the AC power source. The power LED lights. After several seconds, the test LED flashes slowly four times, then stays off.

For each of the four 10BaseT ports on the integrated hub, there is a link/data LED that is lit steadily to indicate a good received link (if a cable is connected to a host or hub) or is flashing to indicate data received on the LAN.

4 Connect the RJ45 plug end of the local manager cable to the RS232 Manager port RJ45 jack on the rear of the modem router.

5 Connect the other end of the manager cable to an RS232 terminal or PC COM port configured for the following communication parameters: 9600 bps, 8, none, and 1.

6 The local maintenance cable connects directly to data terminal equipment (DTE).

Note: The analog telephone line must be either a C.O. line or a PBX extension with a Direct Inward Dialing (DID) number, whichever complies with the customer's network security policy.

End of Procedure

Configure the RM356 modem router by the manager menu

This procedure can be performed from a terminal or PC connected to the local RS232 manager port on the rear of the modem router. Alternatively the manager menu can be accessed by Telnet after the IP addressing and routing have been set up initially from the local manager port.

Use the following keys in the RM356 manager menu:

- the arrow keys to navigate
- the spacebar key to toggle pre-defined configuration values for a field
- the Enter key saves data changes to ROM and exits the current menu
- the Esc key exits the current menu without saving changes
- enter menu selection number when prompted to display a sub-menu, configuration form, or command prompts

Procedure 104
Configuring the RM356 modem router

1. Press the **Enter** key from the terminal or manager menu. The **Enter Password:** prompt is displayed for 10 seconds.
2. Enter the default RM356 manager password **1234**. The **RM356 Main Menu** is displayed. See page 658 for a complete view of the RM356 modem router menus.

```
RM356 Main Menu

  Getting Started                    Advanced Management
    1. General Setup                   21. Filter Set
    2. MODEM Setup                   Configuration
    3. Ethernet Setup
    4. Internet Access Setup           23. System Password
                                       24. System Maintenance
 Advanced Applications
   11. Remote Node Setup
   12. Static Routing Setup
   13. Default Dial-in Setup
   14. Dial-in User Setup              99. Exit

 Enter Menu Selection Number:
```

3 At the **Enter Menu Selection Number:** prompt, enter menu selection number **1** to access the General Setup under **Getting Started**. The **Menu 1 - General Setup** sub-menu is displayed.

```
Menu 1 - General Setup

System Name= Room_304_RCH_Training_Center
Location= Sherman Ave., Richardson, TX
Contact Person's Name= John Smith, 972 555-1212

Press ENTER to Confirm or ESC to Cancel:
```

4 Under General Setup, type in the **System Name** (19 characters, no spaces), **Location**, and **Contact Person's Name** for the Meridian 1 and Succession CSE 1000 site.

Use the up and down arrow keys to move the cursor to the prompt **Press ENTER to Confirm or ESC to Cancel:** at the bottom of the menu. Press **Enter** to confirm and save data to ROM.

5 Enter menu selection number **2** to access the MODEM Setup under the **Getting Started** section. The **Menu 2 - Modem Setup** sub-menu is displayed.

```
Menu 2 - MODEM Setup

Modem Name= MODEM
Active= Yes
Direction= Incoming
Phone Number=
Advanced Setup= No

Press ENTER to Confirm or ESC to Cancel:
```

6 Use the arrow keys to navigate and space bar to toggle values. Type in **Modem Name**. Set **Active= Yes** and **Direction= Incoming**. Type in the modem router's **Phone Number** for reference.

7 Press **Enter** to confirm and save data to ROM.

8 Enter menu selection number **3**, to access Ethernet Set under the **Getting Started** section. The **Menu 3: Ethernet Setup** sub-menu is displayed.

```
Menu 3 - Ethernet Setup

1. General Setup
2. TCP/IP and DHCP Setup

Enter Menu Selection Number:
```

9 Enter menu selection **2**, under **Ethernet Setup**. The **Menu 3.2 - TCP/IP and DHCP Ethernet Setup** is displayed.

```
Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP Setup:
DHCP= None
Client IP Pool Starting Address= N/A
Size of Client IP Pool= N/A
Primary DNS Server= N/A
Secondary DNS Server= N/A

TCP/IP Setup:
IP Address= 47.177.16.254
IP Subnet Mask= 255.255.255.0
RIP Direction= None
Version= RIP-2B

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

10 Under DHCP Setup, toggle **DHCP= None** using the space bar.

Under TCP/IP Setup, type in the **IP Address** and the **IP Subnet Mask** for the modem router's Ethernet interface on the ELAN. Toggle **RIP Direction= None**.

11 Press **Enter** to confirm and save data to ROM, then press **Esc** to return to the RM356 Main Menu.

12 Enter menu selection number **12**, under the **Advanced Applications** section. The **Menu 12 - Static Route Setup** sub-menu is displayed.

```
Menu 12 - Static Route Setup

1. DefaultGW
2. ________
3. ________
4. ________
Enter Menu Selection Number:
```

Note 1: If firewall security is properly configured in the customer's Management GW router, and if the modem router is enabled access over the customer's enterprise network (CLAN) to other IP Telephony nodes on remote ELANs, define a default network route pointing to the Management GW IP address on the local ELAN. Alternatively, define up to four different static network routes or host routes in the modem router to limit routing access from the modem router to the customer's enterprise network (CLAN).

Note 2: To prevent access from the modem router to the customer's enterprise network (CLAN) through the Management GW router on the ELAN, disable RIP by setting **RIP Direction=None**, and remove all static routes or disable a particular static route by setting **Active=No**.

13 Enter menu selection number **1** to edit the first static route. **Menu 12.1 - Edit IP Static Route** is displayed.

```
Menu 12.1 - Edit IP Static Route

Route #: 1
Route Name= DefaultGW
Active= Yes
Destination IP Address= 0.0.0.0
IP Subnet Mask= 0.0.0.0
Gateway IP Address= 47.177.16.1
Metric= 2
Private= No

Press ENTER to Confirm or ESC to Cancel:
```

14 Type in a descriptive **Route Name** using no spaces, for example, DefaultGW. Toggle **Active= Yes/No** for security purposes. The **Gateway IP Address** is the Management GW IP address on the ELAN where the modem router is connected.

15 Press **Enter** to confirm and save data to ROM, then press **Esc** to return from the sub-menu to the RM356 Main Menu.

16 Enter menu selection number **13**, under the **Advanced Applications** section. The **Menu 13 - Default Dial-in Setup** sub-menu is displayed.

```
Menu 13 - Default Dial-in Setup

 Telco Options:                    IP Address Supplied By:
   CLID Authen= None                 Dial-in User= No
                                     IP Pool= Yes
                                     IP Start Addr= 47.177.16.253
  PPP Options:                     Session Options:
   Recv Authen= PAP                  Input Filter Sets=
   Compression= No                   Output Filter Sets=
   Mutual Authen= No                 Idle Timeout= 1200
   PAP Login= N/A
   PAP Password= N/A

 Callback Budget Management:
   Allocated Budget(min)=
   Period(hr)=

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

17 Under Telco Options, toggle **CLIDAuthen= None/Preferred/ Required**. CLID requires a C.O. line subscribed for CLID service where available.

- Preferred means some dial-in user profiles require CLID, but others do not.
- Required means no dial-in call is connected unless CLID is provided and user profiles require CLID for authentication.

Under PPP Options, toggle **Recv Authen= PAP**. Windows 9x Dial-up Networking (DUN) is not compatible with CHAP/PAP or CHAP on the modem router. Calls are disconnected after a few minutes. Toggle **Compression= No**. Windows 9x DUN is not compatible with software compression on the modem router. Calls are randomly disconnected. Toggle **Mutual Authen= No**.

Under IP Address Supplied By, toggle **Dial-in User= No** and **IP Pool= Yes**. For **IP Start Addr=**, type in the ELAN IP address that will be assigned to the Dial-up Networking (DUN) PPP client on the remote OTM 2.0 PC.

Note: The remote OTM PC receives this ELAN IP address when DUN makes a dial-in PPP connection to the modem router. As long as DUN remains connected to the modem router, IP applications on the remote OTM 2.0 PC function as if the PC were located on the customer's ELAN.

Under Session Options, configure **Input Filter Sets=** and **Output Filter Sets=** according to the customer's IP network security policy and practices. The default setting; however, is no Filter Sets. Set **Idle Timeout= 1200**. 1200 seconds provides 20 minutes idle timeout disconnect for remote support purposes.

Press **Enter** to confirm and save data to ROM and then press **Esc** to return from the sub-menu to the main menu.

18 Enter menu selection number **14**, under the **Advanced Applications** section. The **Menu 14 - Dial-in User Setup** is displayed.

```
Menu 14 - Dial-in User Setup

1. itgadmin
2. ________
3. ________
4. ________
5. ________
6. ________
7. ________
8. ________

Enter Menu Selection Number:
```

Note: Up to eight dial-in user profiles can be defined according to the customer's network security policy.

19 Enter menu selection **1** to edit the first dial-in user profile. **Menu 14.1 - Edit Dial-in User** is displayed.

```
Menu 14.1 - Edit Dial-in User

User Name= itgadmin
Active= Yes
Password= ********
Callback= No
Phone # Supplied by Caller= N/A
Callback Phone #= N/A
Rem CLID=
Idle Timeout= 500

Press ENTER to Confirm or ESC to Cancel:
```

20 Type in the **User Name**, such as itgadmin.

21 Toggle **Active= Yes/No** for security purposes.

22 Type in a **Password** for PAP. The DUN client on the remote OTM 2.0 PC must provide the user name and password defined here when dialing up the modem router.

23 Set **Callback= Yes/No** according to the customer's network security policy and practices. Nortel Networks Customer Technical Services (CTS) does not currently accept Callback security calls from the modem router.

24 Set **Rem CLID=** to the **PSTN Calling Number** that is displayed when the remote OTM 2.0 PC dials up the modem router, if CLID authentication is required for the user profile. CLID depends on providing a C.O. line subscribed for CLID service for the modem router's telephone line connection.

25 Set **Idle Timeout= 1200**, where 1200 seconds provides 20 minutes idle timeout disconnect for Nortel Networks remote support purposes.

26 Press **Enter** to confirm and save data to ROM, then press **Esc** to return from the sub-menu to the RM356 Main Menu.

27 Enter menu selection number **23**, under the **Advanced Management** section of the RM356 Main Menu. **Menu 23 - System Password** is displayed.

```
Menu 23 - System Password

Old Password= ?
New Password= ?
Retype to confirm= ?

Enter here to CONFIRM or ESC to CANCEL:
```

28 Type in the **Old Password**. Navigate down and type a **New Password**. Navigate down to **Retype to confirm** and then retype the new password.

Press **Enter** to save the save the changes.

Note: Never leave the RM356 system manager password defaulted to 1234 after the modem router has been installed and configured on the ELAN. The modem router's security features are ineffective if the manager password is not changed on a regular basis according to good network security practices.

End of Procedure

RM356 modem router manager menu description

Application notes on Meridian 1 and Succession CSE 1000 ELAN installation

This section displays the various menus of the RM356 modem router:

```
                         RM356 Main Menu
Getting Started                         Advanced Management
  1. General Setup                   21. Filter Set Configuration
  2. MODEM Setup
  3. Ethernet Setup                   23. System Password
  4. Internet Access Setup            24. System Maintenance

Advanced Applications
  11. Remote Node Setup
  12. Static Routing Setup
  13. Default Dial-in Setup
  14. Dial-in User Setup                  99. Exit

                    Enter Menu Selection Number:

                     Menu 1 - General Setup

               System Name= Room_304_RCH_Training_Center
               Location= Sherman Ave., Richardson, TX
              Contact Person's Name= John Smith, 972 555-1212

               Press ENTER to Confirm or ESC to Cancel:

                     Menu 2 - MODEM Setup

               Modem Name= MODEM
               Active= Yes
               Direction= Incoming
               Phone Number=
               Advanced Setup= No
```

```
Press ENTER to Confirm or ESC to Cancel:

         Menu 3 - Ethernet Setup

1. General Setup
2. TCP/IP and DHCP Setup

      Enter Menu Selection Number:

    Menu 3.1 - General Ethernet Setup

Input Filter Sets= 2
Output Filter Sets=

Press ENTER to Confirm or ESC to Cancel:

Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP Setup:
  DHCP= None
  Client IP Pool Starting Address= N/A
  Size of Client IP Pool= N/A
  Primary DNS Server= N/A
  Secondary DNS Server= N/A

TCP/IP Setup:
  IP Address= 47.177.16.254
  IP Subnet Mask= 255.255.255.0
  RIP Direction= None
    Version= RIP-2B

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

```
                 Menu 12 - Static Route Setup

           1. DefaultGW
           2. ________
           3. ________
           4. ________

                 Enter Menu Selection Number:

               Menu 12.1 - Edit IP Static Route

           Route #: 1
           Route Name= DefaultGW
           Active= Yes
           Destination IP Address= 0.0.0.0
           IP Subnet Mask= 0.0.0.0
           Gateway IP Address= 47.177.16.1
           Metric= 2
           Private= No

           Press ENTER to Confirm or ESC to Cancel:

                Menu 13 - Default Dial-in Setup

 Telco Options:                   IP Address Supplied By:
   CLID Authen= None                 Dial-in User= No
                                     IP Pool= Yes
 PPP Options:                     IP Start Addr= 47.177.16.253
   Recv Authen= PAP
   Compression= No                    Session Options:
   Mutual Authen= No                    Input Filter Sets=
     PAP Login= N/A                     Output Filter Sets=
     PAP Password= N/A                  Idle Timeout= 1200

 Callback Budget Management:
   Allocated Budget(min)=
   Period(hr)=
```

```
                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

                          Menu 14 - Dial-in User Setup

                    1. itgadmin
                    2. ________
                    3. ________
                    4. ________
                    5. ________
                    6. ________
                    7. ________
                    8. ________

                          Enter Menu Selection Number:

                          Menu 14.1 - Edit Dial-in User

                    User Name= itgadmin
                    Active= Yes
                    Password= ********
                    Callback= No
                      Phone # Supplied by Caller= N/A
                      Callback Phone #= N/A
                    Rem CLID=
                    Idle Timeout= 500

                    Press ENTER to Confirm or ESC to Cancel:




                       Menu 21 - Filter Set Configuration
```

```
     Filter                                Filter
     Set #        Comments                 Set #        Comments
    ------  -----------------             ------  -----------------
      1       NetBEUI_WAN                    7      _______________
      2       NetBEUI_LAN                    8      _______________
      3       _______________                9      _______________
      4       _______________               10      _______________
      5       _______________               11      _______________
      6       _______________               12      _______________

                 Enter Filter Set Number to Configure= 0

                 Edit Comments=

                 Press ENTER to Confirm or ESC to Cancel:
```

<u>Menu 21.1 - Filter Rules Summary</u>

```
# A Type                 Filter Rules                       M m n
- - ---- ----------------------------------------------- - - -
1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0              N D N
2 Y IP   Pr=17, SA=0.0.0.0, SP=138, DA=0.0.0.0              N D N
3 Y IP   Pr=17, SA=0.0.0.0, SP=139, DA=0.0.0.0              N D N
4 Y IP   Pr=6, SA=0.0.0.0, SP=137, DA=0.0.0.0               N D N
5 Y IP   Pr=6, SA=0.0.0.0, SP=138, DA=0.0.0.0               N D N
6 Y IP   Pr=6, SA=0.0.0.0, SP=139, DA=0.0.0.0               N D F

               Enter Filter Rule Number (1-6) to Configure:
```

<u>Menu 23 - System Password</u>

```
                 Old Password= ?
                 New Password= ?
                 Retype to confirm= ?
```

```
                Enter here to CONFIRM or ESC to CANCEL:

                     Menu 24 - System Maintenance

                     1.  System Status
                     2.  Terminal Baud Rate
                     3.  Log and Trace
                     4.  Diagnostic
                     5.  Backup Configuration
                     6.  Restore Configuration
                     7.  Software Update
                     8.  Command Interpreter Mode
                     9.  Call Control

                     Enter Menu Selection Number:

                Menu 24.1 -- System Maintenance - Status

Port Status   Speed  TXPkts  RXPkts  Errs  Tx B/s  Rx B/s   Up Time
 1    Idle    0Kbps   16206   12790     0       0       0   0:00:00

     Total Outcall Time:     0:00:00

     Ethernet:                       Name: Room_304_RCH_Traini
       Status:  10M/Half Duplex  RAS S/W Version: V2.13 | 9/25/98
      TX Pkts: 135579          Ethernet Address:00:a0:c5:e0:5b:a6
       RX Pkts: 662866
       Collisions: 49

     LAN Packet Which Triggered Last Call:

                                Press Command:

             COMMANDS: 1-Drop Port 1  9-Reset Counters   ESC-Exit
    Menu 24.2 -- System Maintenance - Change Terminal Baud Rate
```

```
Terminal Baud Rate: 9600

                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

                 Menu 24.3 == System Maintenance - Log and Trace

                    1. View Error Log
                    2. Syslog and Accounting

                             Please enter selection:

   0     179754 PINI  INFO  SMT Session End
   1     179761 PP09  INFO  Password pass
   2     179761 PINI  INFO  SMT Session Begin
   3     179763 PINI  INFO  SMT Session End
   4     179772 PP09  INFO  Password pass
   5     179772 PINI  INFO  SMT Session Begin
   6     179775 PINI  INFO  SMT Session End
   7     179783 PP09  INFO  Password pass
   8     179783 PINI  INFO  SMT Session Begin
   9     179788 PINI  INFO  SMT Session End
  10     179796 PP09  INFO  Password pass
  11     179796 PINI  INFO  SMT Session Begin
  12     179798 PINI  INFO  SMT Session End
  13     179812 PP09  INFO  Password pass
  14     179812 PINI  INFO  SMT Session Begin
  15     179815 PINI  INFO  SMT Session End
  16     179830 PP09  INFO  Password pass
  17     179830 PINI  INFO  SMT Session Begin
  18     179834 PINI  INFO  SMT Session End
```

```
Menu 24.3.2 -- System Maintenance - Syslog and Accounting

           Syslog:
           Active= No
           Syslog IP Address= ?
           Log Facility= Local 1

           Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

```
          Menu 24.4 - System Maintenance - Diagnostic

     MODEM                                 System
       1.  Drop MODEM                        21. Reboot System
       2.  Reset MODEM                       22. Command Mode
       3.  Manual Call
       4.  Redirect to MODEM

     TCP/IP
       11. Internet Setup Test
       12. Ping Host

                 Enter Menu Selection Number:

           Manual Call Remote Node= N/A
           Host IP Address= N/A
```

```
          Menu 24.7 -- System Maintenance - Upload Firmware

           1. Load RAS Code
           2. Load ROM File

                 Enter Menu Selection Number: 1
```

Appendix C: Product Integrity

Contents

This section contains information on the following topics:

Overview

This chapter presents information about the Voice Gateway Media Card's reliability, environmental specifications, and electrical regulatory standards.

Reliability

Reliability is measured by the Mean Time Between Failures (MTBF).

Mean time between failures (MTBF)

The Mean Time Between Failure (MTBF) is 46 years for Voice Gateway Media Cards. Failures per 10^6 hours of operation are 2.483, based on 40 degrees C (140 degrees F).

Voice Gateway Media Card power consumption

The worst case current drawn by the Voice Gateway Media Cards from each Backplane voltage supply is provide in Table 96 on page 668:

Table 96
Voice Gateway Media Card power consumption

Card Type	Power Consumption
ITG-P Line Card	± 15 volt = 19.3 watts => 0.640 amps +5 volt = 10.5 watts => 2.1 amps
Succession Media Card	+ 15 volt = 6 watts => 0.2 amps +5 volt = 7.25 watts => 1.45amps

Environmental specifications

Table 97 shows the environmental specifications of the Voice Gateway Media Card. The Voice Gateway Media Card provides external interface protection to -52 V dc, but does not provide lightning or hazardous voltage protection.

Table 97
Voice Gateway Media Card—environmental specifications

Parameter	Specifications
Operating temperature	0° to +60° C (+32 to +140° F), ambient
Operating humidity	5 to 95% RH (non-condensing)
Storage temperature	–40° to +70° C (–40° to +158° F)

Measurements of performance in regards to temperature and shock were made under test conditions as described in Table 98 on page 670.

Temperature-related conditions

Refer to Table 98 for a display of acceptable temperature and humidity ranges for the Voice Gateway Media Card.

Table 98
Voice Gateway Media Card—environmental specifications

Specification	Minimum	Maximum
Normal Operation		
Recommended	15° C	30° C
Relative humidity	20%	55% (non-condensing)
Absolute	10 ° C	45° C
Relative humidity	20% to	80% (non-condensing)
Short Term (less than 72 hr)	–40° C	70° C
Rate of change	Less than 1° C for every 3 minutes	
Storage		
Recommended	–20° C	60° C
Relative humidity	5%	95% (non-condensing)
	–40° C to 70° C, non-condensing	
Temperature Shock		
In 3 minutes	–40° C	25° C
In 3 minutes	70° C	25° C
	-40° to 70° C, non-condensing	

Electrical regulatory standards

Table 99, Table 100, and Table 101 lists the safety and electro-magnetic compatibility regulatory standards (by geographic region) for the Voice Gateway Media Card.

Specifications for the Voice Gateway Media Card meet or exceed the standards listed in these regulations.

Safety

Table 99 provides a list of safety regulations met by the Voice Gateway Media Card, along with the type of regulation and the country/region covered by each regulation.

Table 99
Safety regulations

Regulation Identifier	Regulatory Agency
UL 1459	Safety, United States, CALA
CSA 22.2 225	Safety, Canada
EN 41003	Safety, International Telecom
EN 60950/IEC 950	Safety, International
BAKOM SR 784.103.12/4.1/1	EMC/Safety (Switzerland)
AS3260, TS001 - TS004, TS006	Safety/Network (Australia)
JATE	Safety/Network (Japan)

Electro-magnetic compatibility (EMC)

Electro-Magnetic Containment (EMC) compliance requirements depend on the regulations in effect for the country where the Meridian 1 and Succession CSE 1000 is located. CISPR 22 Class B defines more stringent EMC limits than CISPR 22 Class A requirements (that is, equipment that meets CISPR 22 Class B exceeds CISPR 22 Class A requirements and can be used globally).

The ITG-P Line Card and the Succession Media Cards are approved for CISPR 22 Class A (and FCC Part 15 Class A) limits and approved to CISPR 22 Class B limits with the following configurations:

- ITG-P Line Card
  - For Option 11C/11C-Mini systems, there is no limit to the number of ITG-P Line Cards (NTVQ55AA) that can be installed on a shelf to meet CISPR 22 Class A (and FCC Part 15 Class A) limits. However, to meet CISPR 22 Class B limits, there is a limit of two cards for each shelf.
  - For Option 51C/61C/81C systems, there is no limit to the number of ITG-P Line Cards (NTVQ55AA) that can be installed on a shelf to meet CISPR 22 Class A (and FCC Part 15 Class A) limits and CISPR 22 Class B limits.
- Succession Media Card
  - For Option 11C/11C-Mini systems, there is no limit to the number of Succession Media cards (NTVQ01BA) that can be installed on a shelf to meet CISPR 22 Class A (and FCC Part 15 Class A) limits and CISPR 22 Class B limits. If the Succession Media Cards (NTVQ01BA) are installed in a shelf that already has ITG-P Line Cards (NTVQ55AA), then the ITG-P Line Card's EMC requirements supersedes the Succession Media Card EMC requirements.

— For Option 51C/61C/81C systems, there is no limit to the number of Succession Media Cards (NTVQ01BA) that can be installed on a shelf to meet CISPR 22 Class A (and FCC Part 15 Class A) limits. To meet CISPR 22 Class B limits, there is a limit of ten Succession Media Cards (NTVQ01BA) that can be installed on one shelf. If the Succession Media cards are to be installed in a shelf that already has ITG-P Line cards (NTVQ55AA), then the ITG-P Line Card's EMC requirements supersedes the Succession Media card EMC requirements.

Table 100 lists Electro-magnetic emissions regulations met by the Voice Gateway Media Card, along with the country's standard that lists each regulation.

Table 100
Electro-Magnetic Emissions

Regulation Identifier	Regulatory Agency
FCC part 15 Class A	United States Radiated Emissions
CSA C108.8	Canada Radiated Emissions
EN50081-1	European Community Generic Emission Standard
EN55022/CISPR 22 CLASS B	Radiated Emissions (Basic Std.)
BAKOM SR 784.103.12/4.1/1	EMC/Safety (Switzerland)
SS-447-20-22	Sweden EMC standard
AS/NZS 3548	EMC (Australia/New Zealand)
NFC 98020	France EMC standard

Table 101 lists Electro-magnetic immunity regulations met by the Voice Gateway Media Card, along with the country's standard that lists each regulation.

Table 101
Electro-Magnetic Immunity

Regulation Identifier	Regulatory Agency
CISPR 22 Sec. 20 Class B	I/O conducted noise
IEC 801-2 (level 4)	ESD (Basic Standard)
IEC 801-3 (level 2)	Radiated Immunity (Basic Standard)
IEC 801-4 (level 3)	Fast transient/Burst Immunity (Basic Standard)
IEC 801-5 (level 4, preliminary)	Surge Immunity (Basic Standard)
IEC 801-6 (preliminary)	Conducted Disturbances (Basic Standard)
BAKOM SR 784.103.12/4.1/1	EMC/Safety (Switzerland)
SS-447-20-22	Sweden EMC standard
AS/NZS 3548	EMC (Australia/New Zealand)
NFC 98020	France EMC standard

Appendix D: Subnet Mask Conversion from CIDR to Dotted Decimal Format

Overview

Subnet masks are expressed in Classless InterDomain Routing (CIDR) format, appended to the IP address, such as 10.1.1.1/20. The subnet mask must be converted from CIDR format to dotted decimal format in order to configure IP addresses.

The CIDR format expresses the subnet mask as the number of bits counting from the most significant bit of the first IP address field. A complete IP address consists of 32 bits. Therefore, a typical CIDR format subnet mask is in the range from /9 to /30. Each decimal number field in the dotted decimal format has a value from 0 to 255, where decimal 255 represents binary 1111 1111.

Procedure 105
Converting subnet mask from CIDR format to dotted decimal format

1 Divide the CIDR format value by 8. The quotient (the number of times that eight divides into the CIDR format value) equals the number of dotted decimal fields containing 255.

In the example above, the subnet mask is expressed as /20. Twenty divided by eight equals a quotient of two, with a remainder of four. Therefore, the first two fields of the subnet mask in dotted decimal format are 255.255.

2 If there is a remainder, refer to Table 102, to obtain the dotted decimal value for the field following the last field containing “255”. In the example of /20 above, the remainder is four. In Table 102, a remainder of four equals a binary value of 1111 0000 and the dotted decimal value of the next and last field is 240. Therefore the first three fields of the subnet mask are 255.255.240.

3 If there are any remaining fields in the dotted decimal format, they have a value of 0. Therefore, the complete subnet mask in dotted decimal format is 255.255.240.0.

End of Procedure

Table 102
CIDR format remainders

Remainder of CIDR format value divided by eight	Binary value	Dotted decimal value
1	1000 0000	128
2	1100 0000	192
3	1110 0000	224
4	1111 0000	240
5	1111 1000	248
6	1111 1100	252
7	1111 1110	254

Appendix E: DHCP Supplementary Information

Contents

This section contains information on the following topics:

Introduction to DHCP

To understand how the i2002 Internet Telephone, i2004 Internet Telephone, and the i2050 Software Phone acquire the needed network configuration parameters automatically, the following section briefly describes the Dynamic Host Configuration Protocol (DHCP). Read this section if you are unfamiliar with the DHCP. Topics discussed are helpful for the configuration and future maintenance of the DHCP server and ensure correct implementation with the i2002 and i2004 Internet Telephones.

DHCP is an extension of BootP. Like BootP, it operates on the client-server model. Unlike BootP, DHCP has more message types. DHCP enables the dynamic allocation of IP addresses to different clients. It can be used to configure clients by supplying the network configuration parameters such as gateway or router IP addresses.

In addition, DHCP has a lease system that controls the duration an IP address is leased to a client. The client can request a specific lease length, or the administrator can determine the maximum lease length. A lease can range from one minute to 99 years. When the lease is up or released by the client, the DHCP server automatically retrieves it and reassigns it to other clients, if necessary. This is an efficient and accurate way to configure clients quickly. This saves the administrator from an otherwise repetitive task. IP addresses can be shared among clients that do not require permanent IP addresses.

DHCP messages

There are seven different DHCP messages. Each message relates certain information between the client and server (see Table 103).

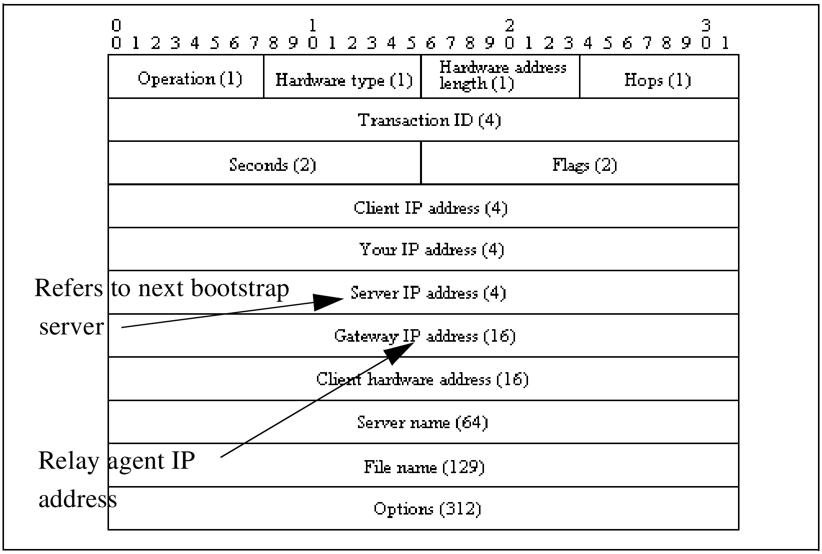
Table 103
DHCP message types

DHCP Message Types	Description
DHCPDISCOVER	Initiates a client request to all servers.
DHCPOFFER	Offer from server following client request.
DHCPREQUEST	Requests a particular server for services.
DHCPAK	Notifies client that requested parameters could be met.
DHCPNAK	Notifies client that requested parameters could not be met.
DHCPDECLINE	Notifies server that offer is unsatisfactory and will not be accepted.
DHCPRELEASE	Notifies server that IP address is no longer needed.

DHCP message format

The DHCP message format shown in Figure 172 on page 680 is common to all DHCP messages. Each message is made of 15 fields, 14 fixed-length fields and one variable length field. The fixed-length fields must be the specified number of bytes as indicated in the brackets. If there is not enough data, or there is no data at all, zeros are used to fill in the extra spaces.

Figure 172
DHCP message format



The Options field is the only field with a variable length. It is optional, but very important as it transports additional network configuration parameters. The DHCP options are the actual subfields that are used in this project.

DHCP message exchange

For a client to receive services from a DHCP server, an exchange of DHCP messages between the client and server must take place. The sequence and types of DHCP message exchanged can differ, but the mechanism of acquiring and supplying information remains the same.

Usually the client initiates the exchange with a DHCP message broadcast. Using a broadcast enables the client to send messages to all servers on the network without having an associated IP address. The broadcast is local to the LAN, unless a DHCP relay agent is present to forward the packet.

At this point, the client has no information about the server or the IP address it is going to receive (unless it is requesting a renewal), so the fields in the DHCP message are empty. However, the client knows its own MAC address and includes it in the Client hardware address field. The client can also have a list of parameters it would like to acquire and can request them from the DHCP server by including the Parameter Request List option (Option Code 55) in the DHCPDISCOVER message.

When the DHCP server sees the broadcast, it responds by broadcasting its own DHCP message. The server, since it knows more about the network, is able to fill in most of the information in the message. For example, information such as server IP address and gateway IP address are included in their respective fields. Since the client does not have an IP address yet, the server uses the client's MAC address to uniquely identify it. When the client sees the broadcast, it matches its MAC address against the one in the message.

Using this method, the server and client can supply or receive information through the exchange of their DHCP messages.

DHCP options

DHCP options are the sub-fields of the Options field. They carry additional network configuration information requested by the client such as IP address lease length and subnet mask.

Each DHCP option has an associated option code and a format for carrying data. Usually the format is as follows:

Option code Length Data

There are two categories of DHCP options, standard and non-standard. The standard options are predefined by the industry, while non-standard options are user-defined to fit the needs of a particular vendor or site.

There are a total of 255 DHCP option codes where option codes 0 and 255 are reserved, 1-77 are predefined, 1-254 can be used for Vendor Specific Options, and 128-254 are designated for Site Specific Options. This arrangement enables future expansion and is used as a guideline for choosing option codes.

Vendor Specific/Encapsulated Option

The Vendor Specific DHCP options are vendor-defined options for carrying vendor-related information. It is possible to override predefined standard options; however, doing so can cause conflict when used with components that follow the industry standard.

A useful option is the standard Vendor Encapsulated option - code 43. It is used to encapsulate other DHCP options as sub-options. For example, Nortel Network's i2004 Internet Telephone requires vendor specific Voice Gateway Media Card information. The vendor, Nortel Networks, decided to carry this information in one of several Site Specific options and then encapsulate it into option 43. Since the information is specific to a Nortel Networks product, it is vendor specific. Once encapsulated, the information appears as one or more sub-options inside option 43, which the Internet Telephones decode.

Site Specific Option

Another way to transport the Voice Gateway Media Card information is through Site Specific options. These are unused DHCP options that have not been predefined to carry standard information. Unlike the Vendor Specific options, the information transported is "site" specific and option codes 128-254 are used for encoding.

For Nortel Network's Internet Telephones, the Voice Gateway Media Card information involves the location of the Voice Gateway Media Card in the network. This varies for different sites and can be implemented in a Site Specific option. If the Vendor Encapsulation option is used, the information is first encoded in a Site Specific option. Nortel Networks has provided a list of five possible Site Specific option codes to implement the Voice Gateway Media Card information. Only one of the five codes needs to be implemented to carry the information, but the choice is to offset the possibility that the option code chosen has been used for other purposes.

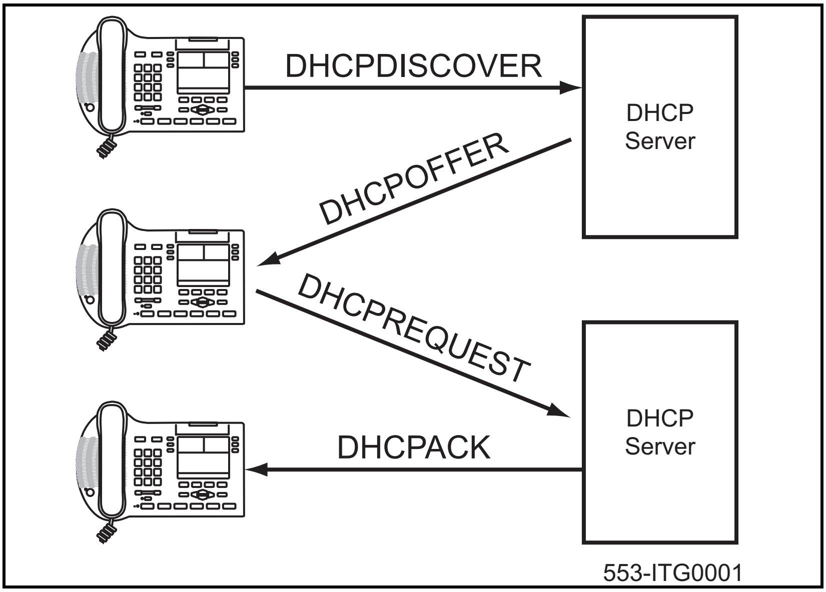
IP Acquisition Sequence

This section focuses on the mechanics and sequence of the DHCP message exchange as the Internet Telephone uses DHCP for IP acquisition. Although the Internet Telephone requests many network configuration parameters as well as an IP address, the following cases focus on the concept of "how" instead of "what" information is acquired. Also, the Internet Telephone is used as the sample client but most of the illustrations apply to other DHCP clients as well.

Case 1

Case 1 is a typical situation where the i2004 Internet Telephone requests services from a DHCP server. This is illustrated in Figure 173 on page 684 and explained below.

Figure 173
IP Acquisition Phase - Case 1



1 The i2004 Internet Telephone initiates the sequence by broadcasting a DHCPDISCOVER message.

2 A DHCP server on the network sees the broadcast, reads the message, and records the MAC address of the client.

3 It checks its own IP address pool(s) for an available IP address and broadcasts a DHCPOFFER message if one is available. Usually the server ARPs or PINGs the IP address to make sure it is not being used.

4 The i2004 Internet Telephone sees the broadcast and after matching its MAC address with the offer, reads the rest of the message to find out what else is being offered.

5 If the offer is acceptable, it sends out a DHCPREQUEST message with the DHCP server's IP address in the Server IP address field.

6 The DCHP server matches the IP address in the Server IP address field against its own to find out to whom the packet belongs.

7 If the IPs match and there is no problem supplying the requested information, the DHCP server assigns the IP address to the client by sending a DHCPACK.

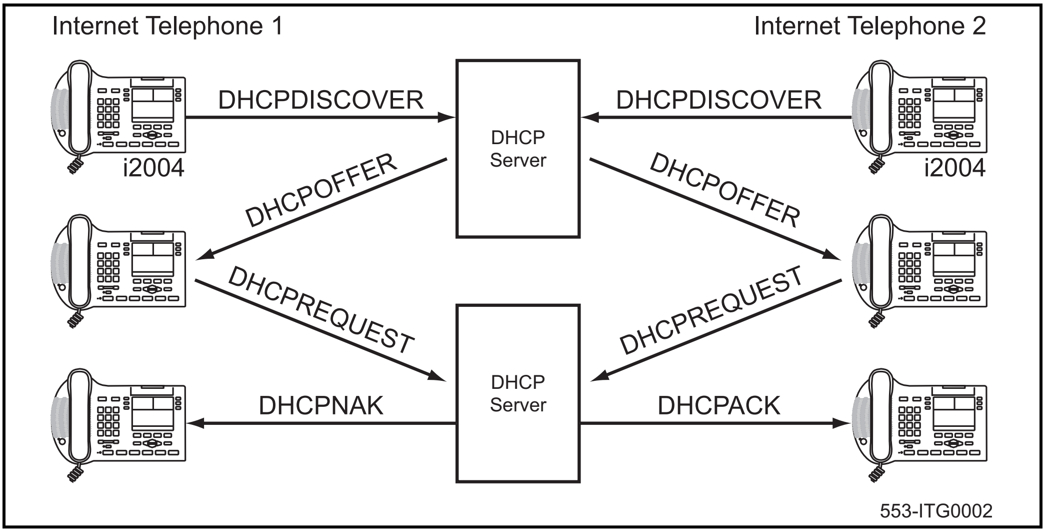
8 If the final offer is not rejected, the IP acquisition sequence is complete.

Case 2

The IP acquisition is unsuccessful if either the server or the client decides not to participate.

- If the DHCP server cannot supply the requested information, it sends a DHCPNAK message and no IP address is assigned to the client. This can happen if the requested IP address has already been assigned to a different client (see Figure 174 on page 686).
- If the Client decides to reject the final offer (after the server sends a DHCPACK message):
  - the Client sends a DHCPDECLINE message to the server, telling it the offer is rejected.
  - the Client must restart the IP acquisition by sending another DHCPDISCOVER message, in search of another offer.

Figure 174
IP Acquisition Sequence - Case 2



Case 3

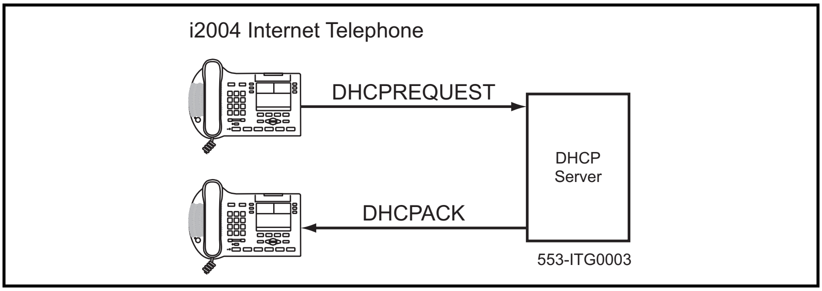
Finally, when a client is finished with a particular IP address, it sends a DHCPRELEASE message to the server which reclaims the IP address. If the client requires the same IP address again, it can initiate the process as follows:

1 i2004 Internet Telephone broadcasts a DHCPREQUEST to a particular DHCP server by including the server's IP address in the Server IP Address field of the message. Since it knows the IP address it wants, it requests it in the DHCP message.

2 The DHCP server sends a DHCPACK message if all the parameters requested are met.

Case 1 is similar to Case 3, except the first two messages have been eliminated. This reduces the amount of traffic produced on the network (see Figure 175 on page 687).

Figure 175
IP Acquisition sequence - Case 3



Multiple DHCPOFFERS

In some networks, if more than one DHCP server is present, a client can receive multiple DHCPOFFER messages. Under these situations, the IP acquisition sequence depends on the client. The client can wait for multiple offers, or access with the first offer it receives. If it accepts multiple offers, it compares them before choosing one with the most fitting configuration parameters. When a decision is made, the message exchange is the same as if there is only one DHCP server and proceeds as in the previous Cases. The servers that have not been chosen to provide the service do not participate in the exchange.

The i2004 Internet Telephone responds only to DHCPOFFERs that have the same unique string identifier, "Nortel-i2004-A", as the i2004 Internet Telephone. This string must appear in the beginning of the list of Voice Gateway Media Card parameters. Without this string, the i2004 Internet Telephone does not accept the DHPCOFFER, even if all parameters requested and Voice Gateway Media Card information are present. If no valid DHCPOFFERs are sent then, the i2004 Internet Telephone keeps broadcasting in search of a valid offer.

With multiple DHCP servers on the same network, a problem can occur if any two of the servers have overlapping IP address range and no redundancy. DHCP redundancy is a property of DHCP servers. This redundancy enables different DHCP servers to serve the same IP address ranges simultaneously. Administrators must be aware that not all DHCP servers have this capability.

Internet Telephone support for DHCP

This section covers the three uses of DHCP (Full, Partial, and VLAN Auto Discovery) by the i2002 and i2004 Internet Telephones.

An "i2004 aware" DHCP server is needed only for the Full DHCP and VLAN Auto discovery. An Internet Telephone can obtain its IP address and subnet mask using Partial DHCP. The "i2004 aware" part returns the Node IP and registration port number. In the case of the DHCP Auto Discovery, it returns the VLAN IDs. Separate DHCP vendor specific entries are needed for the Full DHCP data and the VLAN Auto Discovery data. When using the VLAN Auto Discovery, both Full DHCP and VLAN Auto Discovery must be configured. Full DHCP and Auto VLAN are implemented as separate functions in the Internet Telephone firmware. However, in practice, Full DHCP and Auto VLAN are frequently used together.

Full DCHP

DHCP support in the Internet Telephone includes sending a Class Identifier option with the value "Nortel-i2004-A" in each DHCP Discovery and Request. Additionally, the Internet Telephone checks for either a Vendor Specific option message with a specific, unique to Nortel i2004, encapsulated sub-type, or a Site Specific DHCP option. In either case, an Internet Telephone specific option must be returned by the i2004-aware DHCP server in all DHCPOFFER and DHCPACK messages. The Internet Telephone uses the information returned in this option to configure itself for proper operation. This includes binding a new IP address, netmask, and default gateway (for local IP stack) as well as configuring the primary bootstrap server and optional secondary server.

DHCP support in the Internet Telephone requires sending a “Class Identifier” option with each DHCP Discovery and Request message. Additionally, the telephone checks for either a Vendor Specific option message with a specific, unique to Nortel i2004, encapsulated sub-type, or a Site Specific DHCP option.

In either case, a Nortel i2004-specific option must be returned by the i2004 aware DHCP server in all Offer and Acknowledgement (ACK) messages. The Internet Telephone parses this option’s data and use it to configure the information required to connect to the TPS.

The DHCP response is parsed to extract the Internet Telephone's IP address, netmask, and gateway. The vendor specific field is then parsed to extract the Server 1 (minimum) and optionally Server 2. By default, Server 1 is always assumed to be the "primary" server after a DHCP session.

In order for the Internet Telephone to accept Offers/Acks, they must contain all of the following:

- A Router option (needs a default router to function)
- A Subnet Mask option
- A Vendor Specific option as specified below or a Site Specific option as specified below.

  Note 1: The initial DHCP implementation required only the Vendor Specific encapsulated sub-option. In inter-op testing with Windows NT (up to Service Release 4), it was discovered that Windows NT does not properly adhere to RFC 1541. As a result this option is not possible. The implementation was changed to add support for either Vendor Specific sub-ops or Site Specific options. This new extension has been tested and verified to work with Windows NT.

  Note 2: The site-specific options are all DHCP options between 128 (0x80) and 254 (0xFE). These options are reserved for site specific use by the DHCP RFCs.

Format for Nortel Networks i2004 Terminal DHCP Class Identifier Field

All Internet Telephones (i2002, i2004, and i2050) fill in the Class ID field of the DHCP Discovery and Request messages with:

"**Nortel-i2004-A**", where:

- ASCII encoded, NULL (0x00) terminated
- unique to Nortel i2004
- "-A" uniquely identifies this version

Format for Nortel Networks i2004 Terminal DHCP Encapsulated Vendor Specific Field

This sub-option must be encapsulated in a DHCP Vendor Specific Option (Refer to RFC 1541 and RFC 1533) and returned by the DHCP server as part of each DHCP OFFER and ACK message in order for the Internet Telephone to accept these messages as valid.

The Internet Telephone parses this option's data and use it to configure the information required to connect to the TPS.

> ***Note 1:*** Either this encapsulated sub-option must be present, or a similarly encoded site-specific option must be sent (see below). Configure the DHCP server to send one or the other - not both.

> ***Note 2:*** The choice of using either Vendor Specific or Site Specific options is provided to enable Windows NT DHCP servers to be used with the Internet Telephone. Windows NT servers do not properly implement the Vendor Specific Option and as a result, Windows NT implementations must use the Site Specific version.

Format of the Encapsulated Vendor Specific Sub-option field

The format of the field is:

- **Type (1 octet):** 5 choices: 0x80, 0x90, 0x9d, 0xbf, 0xfb (128, 144, 157, 191, 251). Providing a choice of five types allows the i2004 to work in environments where the initial choice could already be in use by a different vendor. Pick only one TYPE byte.
- **Length (1 octet):** variable - depends on message content.
- **Data (length octets):** ASCII based with the following format:

  "Nortel-i2004 -A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr."

The string "Nortel-i2004 -A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr." is described in Table 104.

Table 104
Encapsulated Vendor Specific Sub-option field

Parameter	Description
Nortel-i2004-A	Uniquely identifies this as the Nortel option Signifies this version of this specification. Future enhancements could use -B
iii.jjj.kkk.lll:ppppp	Identifies IP address:port for server (ASCII encoded decimal)
aaa	Identifies Action for server (ASCII encoded decimal, range 0..255)
rrr	Identifies retry count for server (ASCII encoded decimal, range 0..255). This string can be NULL terminated although the NULL is not required for parsing.
ACSII symbols	The comma "," is used to separate fields The semicolon ";" is used to separate Primary from Secondary server information The period "." is used to signal end of structure

Table 105 on page 691 shows the “pieces” of the Nortel option string. The Nortel designator Nortel-i2004-A is separated from the Connecter Server stings using a comma. The Connect Servers are separated using a semi-colon.

Table 105
Nortel option string

Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr;iii.jjj.kkk.lll:pppp,aaa,rrr.				
Nortel Class Identifier Field	comma	Primary Connect Server	semicolon	Secondary Connect Server
Nortel-i2004-A	,	iii.jjj.kkk.lll:ppppp,aaa,rrr	;	iii.jjj.kkk.lll:ppppp,aaa,rrr

Note 1: "aaa" and "rrr" are ASCII encoded decimal numbers with a range of 0..255. They identify the "Action Code" and "Retry Count", respectively, for the associated TPS server. Internally to i2004 they are stored as 1 octet (0x00..0xFF). Note that these fields must be no more than 3 digits long.

Note 2: The string enables the configuration of information for two Connect Servers. However, only one Connect Server exists for a node. If the Secondary Connect Server portion of the string is specified, then the string information must be the same as the primary Connect Server information. Since only the information for primary Connect Server is required, the primary connect server string can be ended with a period (.) instead of a semi-colon (;). For example, "Nortel-i2004-A,iii.jjj.kkk.lll:ppppp,aaa,rrr."

Note 3: Action code values (0-255):
1 - UNIStim Hello (currently only this type is a valid choice)
all other values (0, 2-255) - reserved

Note 4: iii,jjj,kkk,lll are ASCII encoded, decimal numbers representing the IP address of the server. They do not need to be 3 digits long as the "**.**" and "**:**" delimiters guarantee parsing. For example, '001', '01', and '1' would all be parsed correctly and interpreted as value 0x01 internal to the i2004. Note that these fields must be no more than three digits long each.

Note 5: ppppp is the port number in ASCII encoded decimal. The port number must be set to 4100.

Note 6: In all cases, the ASCII encoded numbers are treated as decimal values and all leading zeros are ignored. More specifically, a leading zero does not change the interpretation of the value to be OCTAL encoded. For example, 0021, 021, and 21 are all parsed and interpreted as decimal 21.

Format for Nortel Networks i2004 Terminal DHCP Site Specific Option

This option uses the "reserved for site specific use" DHCP options (number 128 to 254 - refer to RFC 1541 and RFC 1533) and must be returned by the DHCP server as part of each DHCP OFFER and ACK message for the i2004 to accept these messages as valid.

The Internet Telephone pulls the relevant information out of this option and uses it to configure the IP address and so on for the primary and (optionally) secondary TPS's.

> ***Note 1:*** Either this site specific option must be present or a similarly encoded vendor-specific option must be sent (as described above). For example, configure the DHCP server to send one or the other - not both.

> ***Note 2:*** The choice of using either Vendor Specific or Site Specific options is provided to enable Windows NT DHCP servers to be used with the Internet Telephone. Windows NT servers do not properly implement the Vendor Specific Option and as a result, Windows NT implementations must use the Site Specific version.

Format of the DHCP Site Specific field

The format of the DHCP Site Specific field is same as the format of the Encapsulated Vendor Specific Sub-option field. Refer to "Format of the Encapsulated Vendor Specific Sub-option field" on page 690.

Partial DCHP

Partial DHCP is the default DHCP response from a DHCP server which has not been configured to provide the vendor specific information. Using Partial DHCP, an Internet Telephone can obtain its IP address, subnet mask, and gateway IP address. The remainder of the configuration information is manually entered at the Internet Telephone.

DHCP Auto Discovery

The DHCP server is configured to supply the VLAN information to the i2002 and i2004 Internet Telephones. The server uses the site-specific option in the DHCP offer message to convey the VLAN information to the Internet Telephone.

Configuring a DHCP Server for VLAN Discovery is optional. This configuration is done in addition to any done for Full DHCP configuration and it is required only when configuring the VLAN Auto Discovery.

The following definition describes the Nortel i2004-specific, Site Specific option. This option uses the "reserved for site specific use" DHCP options (DHCP option values 128 to 254) and must be returned by the DHCP server as part of each DHCP OFFER and ACK message for the Internet Telephone to accept these messages as valid. The i2002 and i2004 Internet Telephones pull the relevant information out of this option and uses it to configure itself.

Format of the field

The format of the field is: Type, Length, Data.

Type (1 octet):

There are five choices:

- 0x80 (128)
- 0x90 (144)
- 0x9d (157)
- 0xbf (191)
- 0xfb (251)

Providing a choice of five types enables the i2002 and i2004 Internet Telephones to work in environments where the initial choice is already in use by a different vendor. Select only one Type byte.

Length (1 octet):

This is variable as it depends on message content.

Data (length octets):

ASCII based format: "VLAN-A:XXX+YYY+ZZZ." where,

- "VLAN-A:" - uniquely identifies this as the Nortel DHCP VLAN discovery. Additionally, the "-A" signifies this version of this spec. Future enhancements could use "-B" for example.
- ASCII "+" or "," is used to separate fields.
- ASCII "." is used to signal end of structure.
- XXX, YYY and ZZZ are ASCII encoded decimal numbers with a range of 0-4095. The number is used to identify the VLAN Ids. There are maximum of 10 VLAN Ids can be configured in current version. String “none” or “NONE” means no VLAN (default VLAN).

The DHCP Offer message carrying VLAN information is sent out from the DHCP server without a VLAN tag. However, the switch port adds a VLAN tag to the packet. The packet is untagged at the port of the Internet Telephone.

Appendix F: Setup and Configuration of DHCP Servers

Contents

This section contains information on the following topics:

Installing a Windows NT 4 server

To set up the Windows NT 4 server, follow the instructions provided in the installation booklet. After completion, install Service Pack 3 and make sure the DHCP Manager is included.

WARNING
If you are installing a Windows NT 4 server with Service Pack 4 or later, follow the installation instructions included with your server hardware.

Configuring a Windows NT 4 server with DHCP

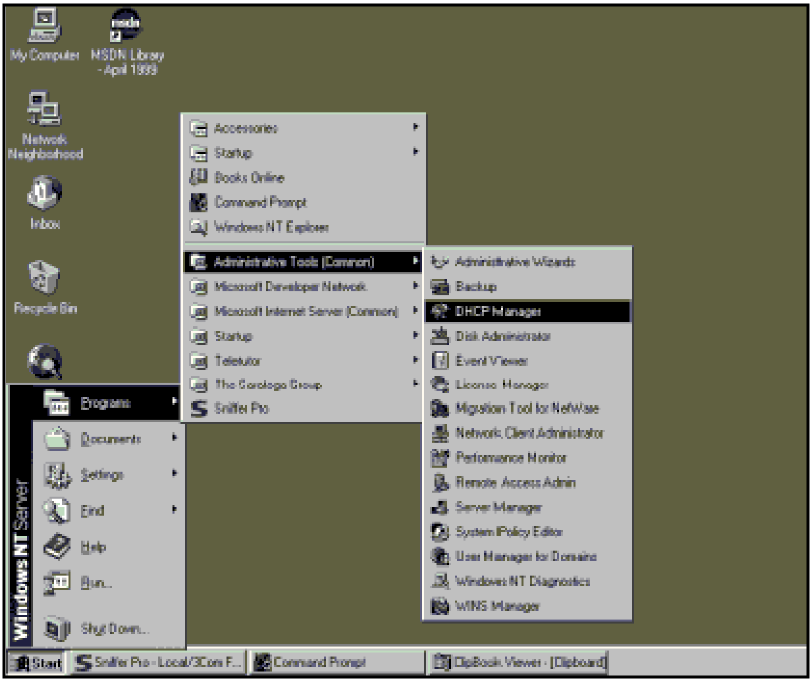
Configure a Windows NT 4 server with DHCP services using the GUI provided.

Procedure 106
Launching the DHCP Manager

1 Click on the Windows **Start** button.

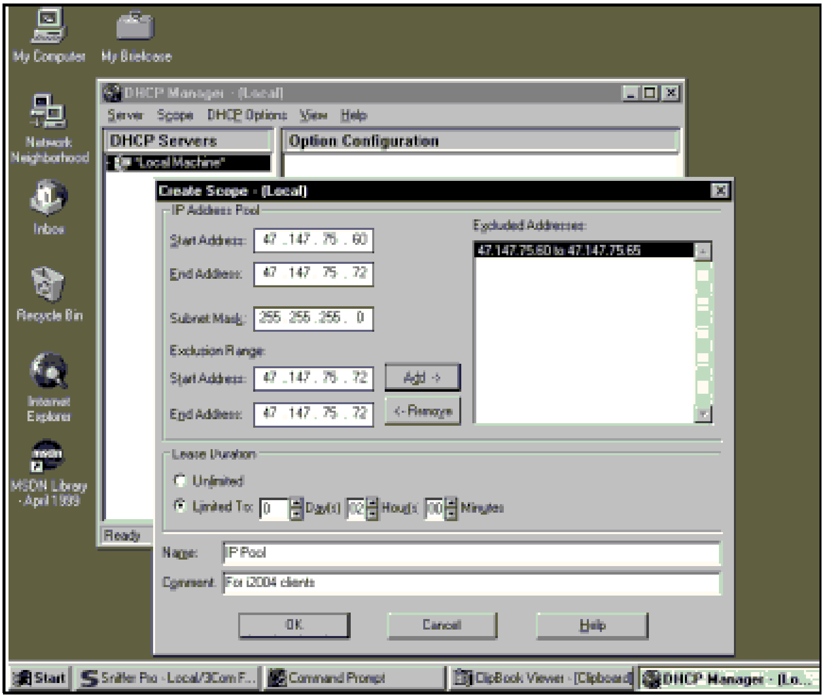
2 Select **Programs | Administrative tools (Common) | DHCP Manager** (see Figure 176 on page 699). The **DHCP Manager** window opens.

Figure 176
Windows NT server screen



3 Double-click **Local Machines** in the left pane. The **Create Scope - (Local)** window opens (see Figure 177 on page 700).

Figure 177
Defining a new scope



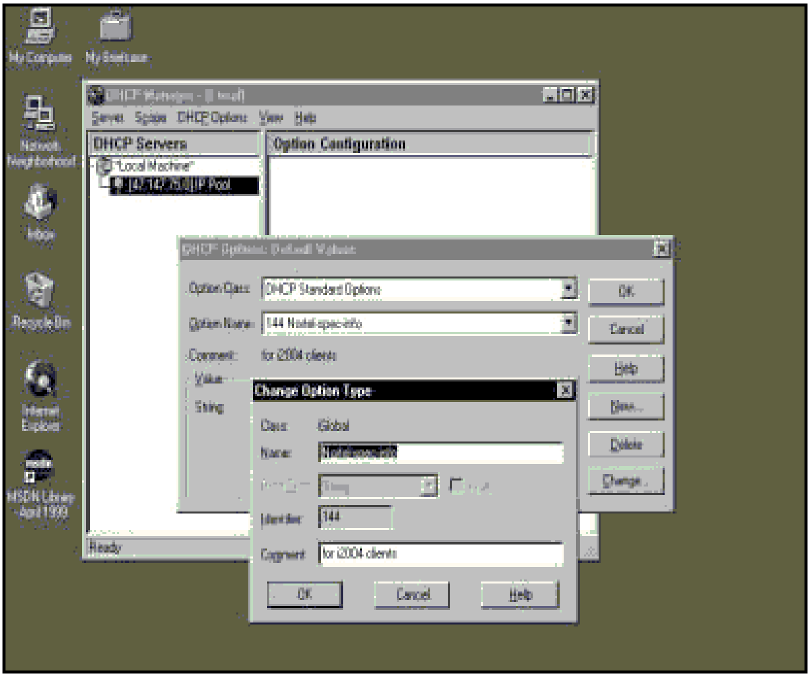
4 Create and then fill in the information. Click **OK** when finished.

5 In the **DHCP Manager - (Local)** window, highlight the scope that serves the i2004 clients.

6 From the **DHCP Options** menu, select **Default Values**. The **DHCP Options - Default Values** window opens.

7 Click the **New** button (see Figure 178 on page 701). The **Change Option Type** window opens.

Figure 178
Defining the Nortel-specific option



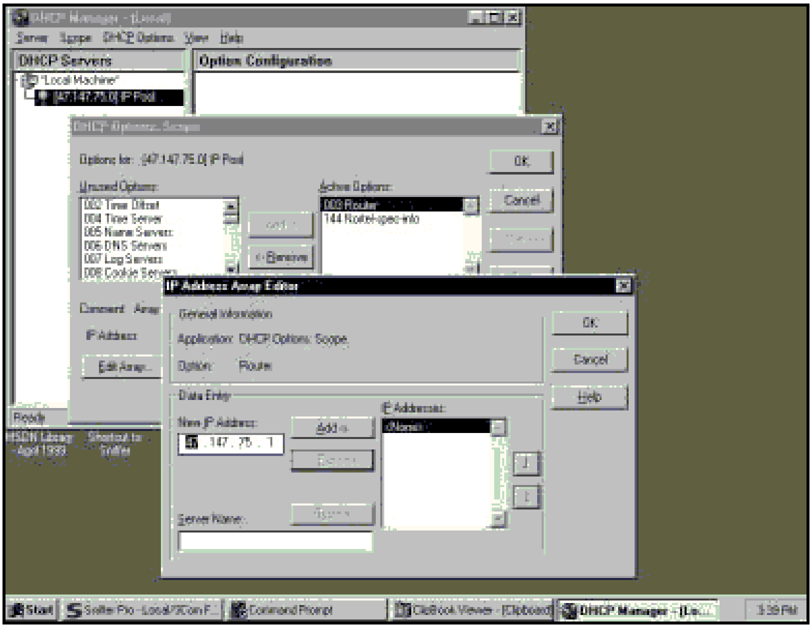
8 Fill in the information and click **OK** when finished. Click **OK** again.

9 From the **DHCP Manager - (Local)** window, highlight the scope to which you want to add DHCP options.

10 From the **DHCP Options** menu, select **Scope**.The **DHCP Options Scope** window opens.

11 Choose standard DHCP options from the left panel and click the **Add ->** button to add them to the right panel. (see Figure 179 on page 702).

Figure 179
Adding standard DHCP options to scope



12 Click the **Edit Array** button. The **IP Address Array Editor** window opens. Edit the default value and then click **OK**. Click OK again.

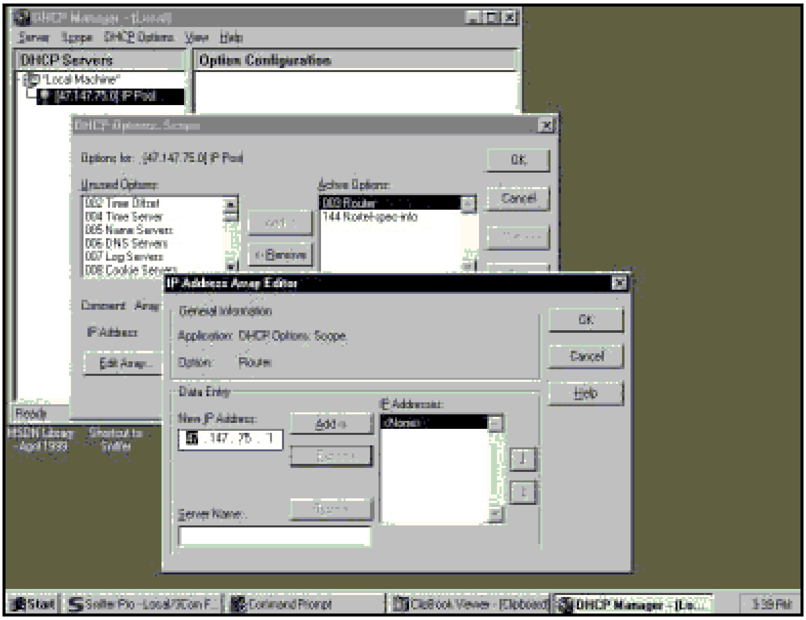
13 From the **DHCP Manager - (Local)** window, highlight the scope that needs to be activated.

14 From the **DHCP Options** menu, select **Scope**. The **DHCP Options Scope** window opens.

15 Click on the **Activate** button.

16 The light bulb next to the scope should turn yellow (see Figure 180 on page 703).

Figure 180
Activating the scope



Note: If DHCP Auto Discovery needs to be configured, see page 694.

End of Procedure

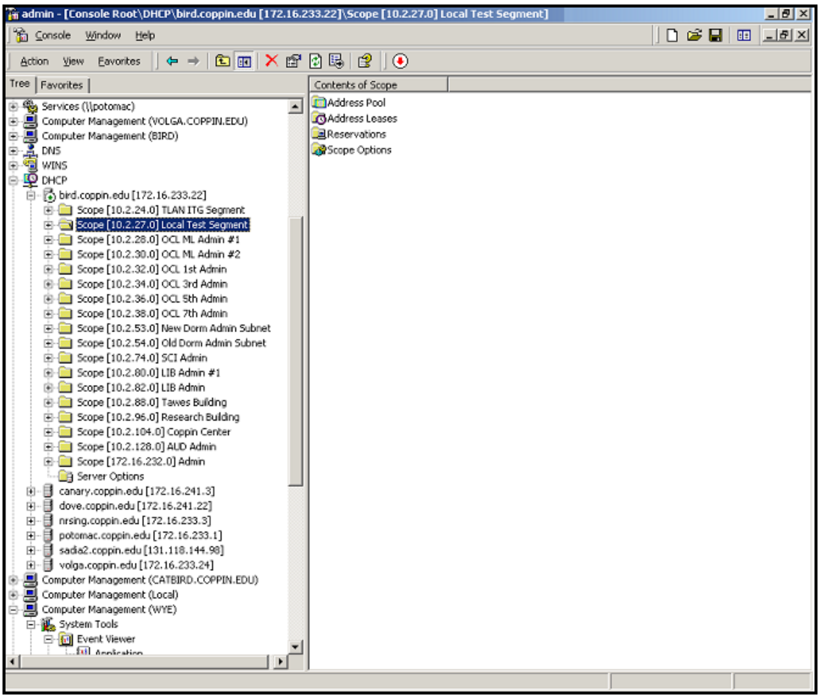
Configuring a Windows 2000 server with DHCP

Configure a Windows NT 4 server with DHCP services using the GUI provided.

Procedure 107
Launching the DHCP Manager

1 Click on the Windows **Start** button. Select **Programs | Administrative Tools | DHCP**. The administrative console window opens (see Figure 181 on page 704).

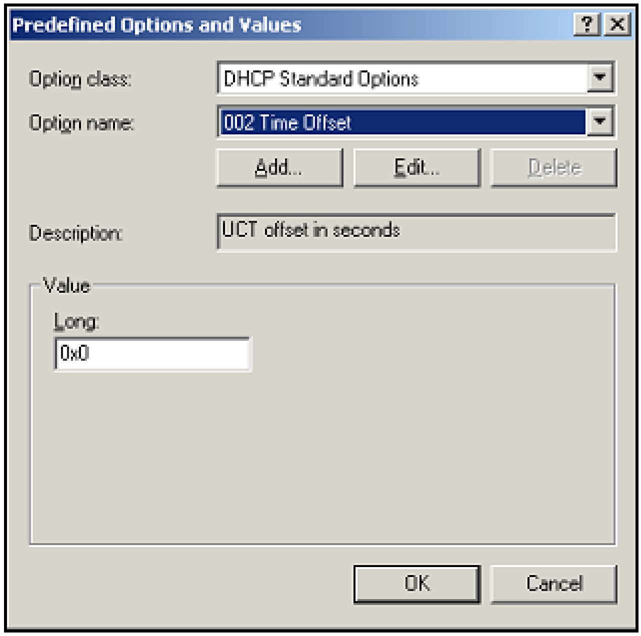
Figure 181
Windows 2000 administration console



2 Highlight DHCP and expand the DHCP option (if it is not already expanded).

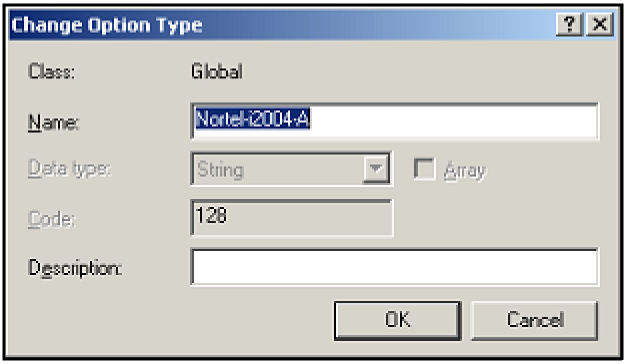
3 Highlight the server and right-click to open the pop-up menu. Select **Set Predefined Options** from the menu. Do not go into the vendor specific settings. The **Predefined Options and Values** window opens (see Figure 182 on page 705).

Figure 182
Predefined Options and Values



4 Click **Add**. The **Change Option Type** window opens (see Figure 183 on page 706).

Figure 183
Change Options Type

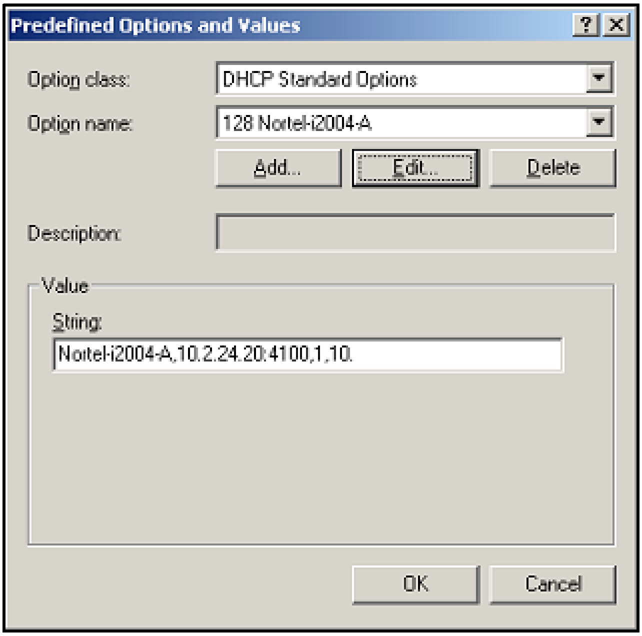


5 Enter a **Name** of your preference. For this example, the name of **Nortel-i2004-A** is entered (see Figure 183).

6 Select **Code** 128.

7 Click **OK** to close the window. The Predefined Options and Values window reopens with the string **128 Nortel-i2004-A** entered in the **Option name** field (see Figure 184 on page 707).

Figure 184
Predefined Options and Values



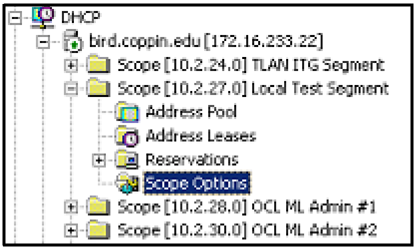
8 Under the **Value** area, enter the following string in the **String** field: **Nortel-i2004-A,x.x.x.x:4100,1,10**; using the following guidelines

- The string is case-sensitive
- Place a period at the end of the string
- Commas are used as separators
- Spaces are not allowed
- x.x.x.x is the IP address of the IP Telephony node
- If it is a BCM, replace the 4100 value with 7000

9 Click **OK**.

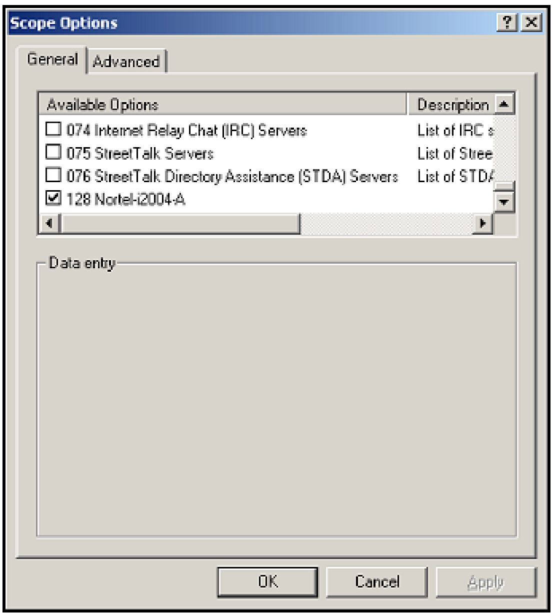
10 The Option Type must now be added to the applicable scopes. Click on the scope **(Scope [x.x.x.x] name)** to expand the scope, then click **Scope Options** (see Figure 185 on page 708).

Figure 185
Scope and Scope Options



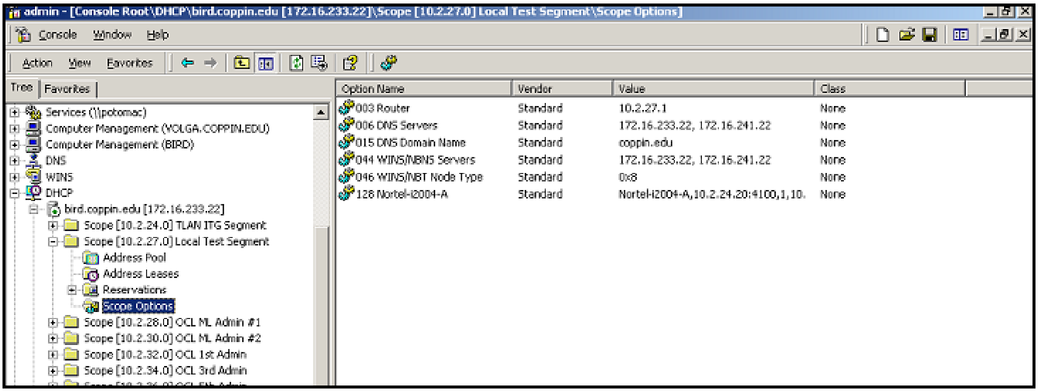
11 The **Scope Options** window opens (see Figure 186). On the General tab, scroll to the bottom of the list and check the **128 Nortel-i2004-A** option.

Figure 186
Scope Options



12 Click **OK**. The Option Name and Value appear in the right pane of the administrative console window (see Figure 187).

Figure 187
Options Name and Value is admin console



Note: If DHCP Auto Discovery needs to be configured, see page 694.

End of Procedure

Installing ISC's DHCP Server

To set up ISC's DHCP server, read the README file and follow the instructions on how to compile, make, and build the server. Once set up is complete, configure the server by following the description in the next section.

CAUTION
Although, Windows NT 4 also has the Vendor Encapsulation Option (option code 43), do not use it to encode the Voice Gateway Media Card information needed by the i2002 and i2004 Internet Telephones. Windows NT 4 enables only 16 bytes of data to be encapsulated which is not enough to encode all the information needed.

Window NT 4's DHCP server transmits any user-defined option associated within a scope if the client requests it. It does not have the ability to distinguish among different types of clients, hence it cannot make decisions based on this information. It is impossible to create a client-specific IP address pool/scope.

Configuring ISC's DHCP Server

To configure ISC's DHCP server, a text based configuration process is used. Configuration is done by adding definitions and declarations in the dhcpd.conf file located at /etc/. Various "man" files are provided on how to configure the server, configure the lease system, use options and conditions, and run the server. Obtain the dhcpd.conf.man5 file in the server directory and read it carefully. It provides explanations on relevant topics, as well as the location of other man files to read for additional information.

Configuring ISC's DHCP to work with the i2004 telephone

Use Procedure 108 on page 711 to configure the ISC's DHCP to work with the i2002 and i2004 Internet Telephones.

There is a particular format for encoding the Voice Gateway Media Card information. In addition to the configuration statements provided, other network and subnet declarations must also be included in the configuration file.

As indicated in the beginning of this section, read the man files and use "Example 1: Configuration file" on page 713 on to configure ISC's DHCP server to work with the i2002 and i2004 Internet Telephones. Also, a copy of the configuration file used for this project is provided at the end of this section.

Procedure 108
Configuring ISC's DHCP server

1 Configure the server to identify a client correctly as the i2002 or i2004 Internet Telephone. This is done using a **match** statement with a conditional **if** enclosed inside a **class** declaration, as follows:

```
class "i2004-clients"{

match if option vendor-class-identifier =
4e:6f:72:74:65:6c:2d:69:32:30:30:34:2d:41:00;}
```

The Hex string represents the text string "Nortel-i2004-A". If the vendor-class-identifier obtained from the client's DHCPDISCOVER message match this Hex-encoded string, then the server adds this client to the "i2004-clients" class. Once a client is classified as a member of a class it must follow the rules of the class.

2 Declare a pool of IP addresses exclusively for the members of the "i2004-clients" class. The pool declaration is used to group a range of IP addresses together with options and parameters that apply only to the pool.

3 Restrict access to the pool. Use the **allow** or **deny** statement to include or exclude the members of a particular class. For example, the follow configuration code enables only members of “i2004-clients” to use this IP address pool:

```
pool{
        allow members of "i2004-clients";
        range 47.147.75.60 47.147.75.65;
        option routers 47.147.75.1;

        # Nortel Networks special string
option vendor-encapsulated-options 80:3d:4e:6f:72:…;}
```

Note: If a client is not a member of this class, it is not assigned an IP address from this pool even if there were no other available IP addresses.

4 The DHCPOFFER from the ISC server must include the Voice Gateway Media Card information if the client is an i2002 or i2004 Internet Telephone. There are two methods to encode the necessary information for the i2004 client:

a. Use the **vendor-encapsulated-options** option (as in the previous example) to encode the information as a sub option.

b. Define a **Site Specific option** to carry the necessary information. To define a site specific option:

— give a declaration in the form of the name of the option, the option code, and the type of data it carries outside any pool or network declarations. For example:

option nortel-specific-info code 144 = string;

— replace the vendor-encapsulated option inside the pool statement with the definition,

option nortel-specific-info = “Nortel …”;

Note: If DHCP Auto Discovery needs to be configured, see page 694.

End of Procedure

Example 1: Configuration file

The following format must be used for encoding the Voice Gateway Media Card information. In addition to the configuration statements provided, other network and subnet declarations must also be included in the configuration file. As mentioned in the beginning of this section, read the man files and use the following example as a guideline:

 # File name: dhcpd.conf

 # Location: /etc/

 # Description: Configuration file for ISC dhcpd server

 # Author: Cecilia Mok

 # Date: September 24, 1999

```
# Global option definitions common for all supported networks...

default-lease-time 300;

max-lease-time 7200;

option subnet-mask 255.255.255.0;

option broadcast-address 255.255.255.255;

# Defining nortel-specific option for i2004 client

option my-vendor-specific-info code 144 = string;

# Declaring a class for i2002 and i2004 clients.
```

```
# Add new clients to the class if their Class Identifier match the special i2004
ID string.

class "i2004-clients"

{

        match if option vendor-class-identifier =
        4e:6f:72:74:65:6c:2d:69:32:30:30:34:2d:41:00;

}



# Declaring another class for PC clients

class "pc-clients"

{}



# Declaring a shared network

# This is to accommodate two different subnets on the same

# physical network; see dhcpd.conf.man5 for more details



shared-network "myNetwork"

{

        # Declaring subnet for current server

        subnet 47.147.77.0 netmask 255.255.255.0

        {}
```

```
# Declaring subnet for DHCP clients
        subnet 47.147.75.0 netmask 255.255.255.0
        {
        # Pool addresses for i2004 clients
        pool
        {
        allow members of "i2004-clients";
        range 47.147.75.60 47.147.75.65;

        option routers 47.147.75.1;

        # Nortel Networks special string
        option nortel-specific-info = “Nortel…”;
}
        default-lease-time 180;
        max-lease-time 300;
}
}
```

Finally, before starting the server, create a blank dhcpd.leases file in the /etc/ directory, which is the same location as the dhcpd.conf file. To start the server, go to /var/usr/sbin/ and type:

```
./dhcpd
```

To run in debug mode, type:

```
./dhcpd –d –f
```

Installing and configuring a Solaris 2 server

Installing a Solaris 2 Server

To set up the Solaris 2 server, consult the accompanying manual and online documentation.

Configuring a Solaris 2 server

Use Procedure 109 on page 716 to configure Solaris 2 with DHCP.

Procedure 109
Configuring a Solaris 2 server

1 Read the man pages listed below:

- dhcpconfig
- dhcptab
- in.dhcpd

Note: There are directions at the end of each page referring to other sources that are helpful.

2 Collect information about the network such as subnet mask, router/gateway and DNS server IP addresses as specified. Make sure this information is current.

3 Log on as **root** and invoke the interface by typing **dhcpconfig** at the prompt. A list of questions is presented and the administrator must supply answers, that are then used to configure the DHCP server.

Note: Solaris 2 uses a text-based interface for configuring DHCP services.

Note: If DHCP Auto Discovery needs to be configured, see page 694.

End of Procedure

Procedure 110
Configuring Solaris 2 to work with i2002 and i2004 Internet Telephones

1 Create a symbol definition for defining a Site Specific option by typing the following in the dhcptab configuration table located at /etc/default/dhcp:

NI2004 s Site,128,ASCII,1,0

Or

2 Use the dhtadm configuration table management utility by typing the following command at the prompt:

dhtadm -A -s NI2004 –d 'Site,128,ASCII,1,0'

where,

NI2004: symbol name

s: identify definition as symbol

Site: site specific option

128: option code

ASCII: data type

1: granularity

0: no maximum size of granularity, that is, infinite

3 Create a Client Identifier macro by entering in the following:

Nortel-i2004-A   m:NI2004="Nortel…":

Or

4 Use the dhtadm command:

dhtadm -A -m Nortel-i2004-A -d   ‘:NI2004=”Nortel…”:’

5 Invoke the DHCP services on the Solaris server by entering at the prompt.:

in.dhcpd,

Specify –d and/or –v options for debug mode. See man page in.dhpcd for more details.

End of Procedure

An example of the tables used in this project is as follows:

DhcptabTable

Locale m :UTCoffst=18000:

nbvws286 m
:Include=Locale:LeaseTim=150:LeaseNeg:DNSdmain=ca.nortel.com:/

DNSserv=47.108.128.216 47.211.192.8 47.80.12.69:

47.147.75.0 m :NISdmain=bvwlab:NISservs=47.147.64.91:

47.147.64.0 m
:Broadcst=47.147.79.255:Subnet=255.255.240.0:MTU=1500:/

Router=47.147.64.1:NISdmain=bvwlab:NISservs=47.147.64.91:

#

NI2004 s Site,128,ASCII,1,0

Nortel-i2004-A m
:NI2004="Nortel-i2004-A,47.147.75.31:4100,1,5;47.147.77.143:4100,1,5.":

Network Table

01006038760290 00 47.147.65.198 47.147.74.36 944600968 nbvws286

0100C04F662B6F 00 47.147.65.199 47.147.74.36 944600959 nbvws286

Appendix G: Downloading IP Line files from Nortel Networks Web Site

Contents

This section contains information on the following topics:

Overview

This appendix provides instruction for downloading files from the Nortel Networks Web site.

Downloading files from Nortel Networks Web site

Follow the steps in Procedure 111 to download IP Line-related loadware and firmware files from the Nortel Networks Web site.

Procedure 111
Downloading files from the Nortel Networks Web site

1 Connect to **http://www.nortelnetworks.com** using any PC with Internet access.

2 Click on the **Downloads** link under the **Support** section at the left of the page. The **Software Downloads** page opens.

3 On the Software Downloads page, under the blue **Product Selection** bar on the right side of the page, click the **View by a Product** link. The **Product Select** page opens.

4 For Meridian 1 and Succession CSE 1000 Rel 1.1 systems:

a. On the Product Select page, select **Internet Telephony Gateway** from the drop-down list, and click **Save**.

b. Select the file from the **Software Downloads** page. The **Software Downloads** page opens with the **Active product: Internet Telephony Gateway** product list displayed. This product list includes the following:

— IP LIne 3.0 (this *.zip file contains IP Line 3.0 loadware, the Internet Telephone firmware, and a readme.txt file)

— Succession Media Card firmware

— ITG-P Line Card firmware

5 For Succession CSE 1000 Rel 2.0 systems:

a. On the Product Select page, select **Succession Communication Server for Enterprise 1000** from the drop-down list, and click **Save**.

b. Select the file from the **Software Downloads** page.The **Software Downloads** page opens with the **Active product: Succession Communication Server for Enterprise 1000** product list displayed. This product list includes the following:

— IP LIne 3.0 loadware and Internet Telephone firmware are contained on the Signaling Server CD-ROM image file

— Succession Media Card firmware

— ITG-P Line Card firmware

6 Click the file to be downloaded.

7 If you are not already logged into your My Nortel Networks account, enter your User ID and Password on the **Sign In** page and then click **Sign In**.

8 If you are not registered to access this Web site, refer to the Meridian 1 or Succession CSE 1000 product bulletin for directions on how to register.

9 Once logged in, ignore the security alert.

10 The **Software Downloads: Software Details Information** page appears. Click the link next to **File Download**.

11 In the **Save As** window, choose the desired path to save the file to local disk on the PC and click **Save**.

End of Procedure

Index

Meridian 1 and Succession Communication Server for Enterprise 1000

IP Line

Description, Installation, and Operation

Publication number: 553-3001-204
Document release: Standard 4.00
Date: November 2002
Printed in Canada

NORTEL NETWORKS™